

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2001 年 6 月 14 日 (14.06.2001)

PCT

(10) 国際公開番号
WO 01/43342 A1

- (51) 国際特許分類: H04L 9/32, G06F 12/14, G10K 15/02, G06F 13/00
- (21) 国際出願番号: PCT/JP00/08593
- (22) 国際出願日: 2000 年 12 月 5 日 (05.12.2000)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願平 11/346861 1999 年 12 月 6 日 (06.12.1999) JP
- (71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP). 株式会社 ビーエフユー (PFU LIMITED) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町宇野気又98番地の2 Ishikawa (JP). 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP).

- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 堀 吉宏 (HORI, Yoshihiro) [JP/JP]. 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP). 高橋政孝 (TAKAHASHI, Masataka) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町宇野気又98番地の2 株式会社 ビーエフユー内 Ishikawa (JP). 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 吉岡 誠 (YOSHIOKA, Makoto) [JP/JP]. 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 利根川忠明 (TONEGAWA, Tadaaki) [JP/JP]; 〒187-8588 東京都小平市上水本町五丁目20番1号 株式会社日立製作所 半導体グループ内 Tokyo (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (P).

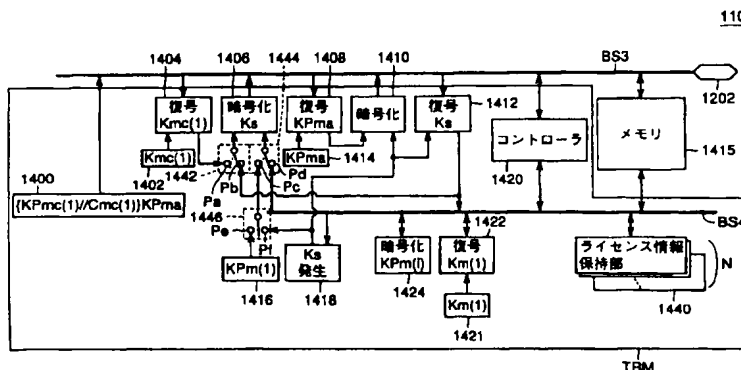
- (74) 代理人: 深見久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU,

[続葉有]

(54) Title: DATA DISTRIBUTION SYSTEM AND RECORDER FOR USE THEREIN

(54) 発明の名称: データ配信システムおよびそれに使用される記録装置





LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL,
PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ,
UA, UG, US, UZ, VN, YU, ZA, ZW.

添付公開書類:
— 国際調査報告書

- (84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

メモ리카ード(110)は、TRM領域内のライセンス情報保持部(1440)にアクセス制限情報(AC1)を格納する。アクセス制限情報(AC1)は、再生可能回数および所有ライセンス数等の情報を有する。コントローラ(1420)は、コンテンツの再生および移動動作時においては、アクセス制限情報(AC1)を確認した上で、再生および移動を実行し、実行後は必要に応じて、アクセス制限情報(AC1)を更新してライセンス情報保持部(1440)に格納する。

明細書

データ配信システムおよびそれに使用される記録装置

5 技術分野

本発明は、携帯電話機等の端末に対して情報を配送するためのデータ配信システムに関し、より特定的には、コピーされた情報に対する著作権保護を可能とするデータ配信システムおよび当該システムで使用されるメモリカードに関するものである。

10

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

15

このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

したがって、このような情報通信網上において音楽データや画像データ等の著作
20 者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、コ
25 ンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディス

ク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

- 5 しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化のほとんどないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽データをコピーすることは、著作権保護のために機器の構成上できないようになっている。

10 このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

 この場合、情報通信網を通じて公衆に送信されるコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

15

発明の開示

 この発明の目的は、情報通信網、たとえば携帯電話機等の情報通信網を介してコンテンツデータを配信することが可能なデータ配信システムおよび当該データ配信システムで使用される記録装置、詳しくはメモリカードを提供することである。

20

 この発明の他の目的は、配信されたコンテンツデータが、著作権者の許可なく複製されることを防止することが可能なデータ配信システムおよび当該データ配信システムで使用される記録装置、詳しくはメモリカードを提供することである。

25 この発明に従うデータ配信システムは、複数の端末と、コンテンツ供給装置とを備える。コンテンツ供給装置は、外部との間でデータを授受するための第1のインタフェース部と、配信が要求された場合において、アクセス制限情報を生成して、少なくともライセンスキーを含む再生情報とアクセス制限情報とを第1のインタフェース部を介して出力するための配信制御部とを含む。各端末は、外部との間でデータを授受するための第2のインタフェース部と、第2のインタフェ

ース部を介して、暗号化コンテンツデータと再生情報とアクセス制限情報とを受けて記録する配信データ解読部とを含む。配信データ解読部は、暗号化コンテンツデータ、再生情報およびアクセス制限情報を記録するための記憶部と、外部から再生情報の出力が指示された場合に、記憶部に記録されたアクセス制限情報に基づいて出力の可否を判断する制御部とを有する。

好ましくは、各端末は、コンテンツ再生部をさらに含み、コンテンツ再生部は、外部からコンテンツデータの再生動作が指示された場合において、配信データ解読部から再生情報および暗号化コンテンツデータを受けて、ライセンスキーによって暗号化コンテンツデータを復号して再生するコンテンツデータ再生部を有する。アクセス制限情報は、配信データ解読部からコンテンツ再生部への、再生情報の出力回数を制限する再生制御情報を含む。制御部は、再生動作が指示された場合において、再生制御情報に基づいて再生情報の出力の可否を判断し、再生情報の出力後に必要に応じて再生制御情報を更新する。

好ましくは、アクセス制限情報は、配信データ解読部から他の配信データ解読部に対しての、再生情報の複製可能回数を制限する複製制限情報を含む。制御部は、他の配信データ解読部に対して再生情報を複製する複製動作が外部から指示された場合において、複製制限情報に基づいて再生情報の出力の可否を判断し、再生情報の出力後において、必要に応じて所有ライセンス数情報を更新可能である。

このようなデータ配信システムにおいては、再生可能回数や所有ライセンス数に関するアクセス制限情報を、配信サーバを介さずに、配信データ解読部、より詳しくはメモ리카ードの内部において、保持および更新できる。したがって、ファイルシステムやアプリケーションプログラム等によって上位レベルからアクセス制限情報を改ざんすることができない構成とすることができる。この結果、再生情報として再生回路の制限付き再生権の発行が可能となり、試験用としての音楽データ（コンテンツデータ）の配布、安価な再生回数制限付き販売等が、さらには、複数の再生権の配信によって集団購入等のサービスが提供できるようになり、利用者にとって利便性の高いデータ配信システムを提供できるとともに、著作権の保護に対して十分なセキュリティー強度を確保できるため、著作権者の権

利をも守ることができるようになる。

この発明の別の局面に従うと、記録装置は、インタフェース部と、記憶部と、制御部とを備える。インタフェース部は、外部との間でデータを授受する。記憶部は、インタフェース部を介して入力される、格納データおよび格納データの記録装置からの出力を制御するためのアクセス制限情報（AC1）を記録する。制御部は、外部から格納データの出力が指示された場合に、アクセス制限情報に基づいて出力の可否を判断する。

好ましくは、アクセス制限情報は、記録装置から他の機器への格納データの出力回数を制限する出力回数制御情報を含み、制御部は、他の機器に対する格納データの出力が指示された場合において、出力回数制御情報に基づいて出力の可否を判断するとともに、出力後に必要に応じて出力回数制御情報を更新可能である。

好ましくは、アクセス制限情報は、他の記録装置に対する格納データの複製可能回数を制限する複製制限情報を含み、制御部は、他の記録装置に対する格納データの複製指示が外部から指示された場合において、所有ライセンス数情報に基づいて格納データの出力の可否を判断し、出力後において、必要に応じて複製制限情報を更新可能である。

このような記録装置においては、複製制限情報および出力回数制御情報といったアクセス制限情報を、配信サーバを介さずに記憶領域内部で保持および更新することができる。したがって、ファイルシステムやアプリケーションプログラム等によって上位レベルからアクセス制限情報を改ざんすることができない構成とすることができる。この結果、再生回路の制限付き再生権の発行が可能となり、試聴用としての音楽データ（コンテンツデータ）の配布、安価な再生回数制限付き販売等が、さらには、複数の再生権の配信によって集団購入等のサービスが提供できるようになり、利用者にとって利便性の高いデータ配信システムを提供できるとともに、著作権の保護に対して十分なセキュリティー強度を確保できるため、著作権者の権利をも守ることができるようになる。

図面の簡単な説明

図1は、本発明のデータ配信システムの全体構成を概略的に説明するための概

念図である。

図 2 は、実施の形態 1 に従うデータ配信システムにおいて使用される通信のためのデータ、情報等の特性を説明する図である。

図 3 は、実施の形態 1 に従うデータ配信システムにおいて使用される鍵データ等の特性をまとめて説明する図である。

図 4 は、図 1 に示されたライセンスサーバの構成を示す概略ブロック図である。

図 5 は、図 1 に示された携帯電話機の構成を示す概略ブロック図である。

図 6 は、図 5 に示されたメモリカードの構成を示す概略ブロック図である。

図 7 は、ライセンス情報保持部に格納される情報の構成を説明する概念図である。

図 8 は、アクセス制限情報 AC 1 の内容を説明する図である。

図 9 は、実施の形態 1 に従うデータ配信システムにおける配信セッション時の動作を説明するための第 1 のフローチャートである。

図 10 は、実施の形態 1 に従うデータ配信システムにおける配信セッション時の動作を説明するための第 2 のフローチャートである。

図 11 は、実施の形態 1 に従う再生セッション時の動作を説明するためのフローチャートである。

図 12 は、実施の形態 1 に従う 2 つのメモリカード間の複製セッション時の動作を説明するための第 1 のフローチャートである。

図 13 は、実施の形態 1 に従う 2 つのメモリカード間の複製セッション時の動作を説明するための第 2 のフローチャートである。

図 14 は、実施の形態 1 に従う 2 つのメモリカード間の複製セッション時の動作を説明するための第 3 のフローチャートである。

図 15 は、実施の形態 2 に従うライセンスサーバの構成を示す概略ブロック図である。

図 16 は、実施の形態 2 に従う携帯電話機の構成を示す概略ブロック図である。

図 17 は、実施の形態 2 に従うデータ配信システムにおける配信動作を説明するためのフローチャートである。

図 18 は、実施の形態 2 に従う再生動作を説明するフローチャートである。

図 1 9 は、実施の形態 2 に従うデータ配信システムにおける 2 つのメモリカード間の複製セッション時の動作を説明するための第 1 のフローチャートである。

図 2 0 は、実施の形態 2 に従うデータ配信システムにおける 2 つのメモリカード間における複製セッション時の動作を説明する第 2 のフローチャートである。

5 図 2 1 は、実施の形態 3 に従うメモリカードの構成を示す概略ブロック図である。

図 2 2 は、再生情報保持部およびライセンス情報保持部に格納される情報の構成を説明する概念図である。

10 発明を実施するための最良の形態

以下、この発明の実施の形態によるデータ配信システムおよび記録装置を図面を参照して詳しく説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

15 なお、以下では携帯電話網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとりて説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他のコンテンツデータ、たとえば画像データ、映像データ、教材データ、テキストデータ、朗読（音声）データ、ゲームプログラム等のコンテンツデータを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

20 （実施の形態 1）

図 1 を参照して、著作権の存在する音楽情報を管理するライセンスサーバ 1 0 は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア 2 0 である携帯電話会社に、このような暗号化コンテンツデータを与える。一方、認証サーバ 1 2 は、音楽データの配信を求めてアクセスしてきた携帯電話ユーザの携帯電話機およびメモリ

25 カードが正規の機器であるか否かの認証を行なう。

配信キャリア 2 0 は、自己の携帯電話網を通じて、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバ 1 0 に中継する。ライセンスサーバ 1 0 は、配信リクエストがあると、認証サーバ 1 2 により携帯電話ユーザの携

携帯電話機およびメモ리카ード等が正規の機器であることを確認し、要求されたコンテンツデータをさらに暗号化した上で配信キャリア 20 の携帯電話網を介して、各携帯電話ユーザの携帯電話機に対してコンテンツデータを配信する。

図 1 においては、たとえば携帯電話ユーザ 1 の携帯電話機 100 には、着脱可能なメモ리카ード 110 が装着される構成となっている。メモ리카ード 110 は、
5 携帯電話機 100 により受信された暗号化コンテンツデータを受取って、上記配信にあたって行なわれた暗号化については復号した上で、携帯電話機 100 中の音楽再生部（図示せず）に与える。

さらに、たとえば携帯電話ユーザ 1 は、携帯電話機 100 に接続したヘッドホン 130 等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。
10

以下では、このようなライセンスサーバ 10 と認証サーバ 12 と配信キャリア 20 と併せて、配信サーバ 30 と総称することにする。

また、このような配信サーバ 30 から、各携帯電話機等にコンテンツデータを
15 伝送する処理を「配信」と称することとする。

このような構成とすることで、まず、メモ리카ード 110 を利用しないと、配信サーバ 30 からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

しかも、配信キャリア 20 において、たとえば 1 曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア 20 が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。
20

しかも、このようなコンテンツデータの配信は、携帯電話機網というクローズなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。
25

このとき、たとえばメモ리카ード 112 を有する携帯電話ユーザ 2 が自己の携帯電話機 102 により、配信サーバ 30 から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量の情報量を有するコンテンツデータ

等を携帯電話ユーザ 2 が直接配信サーバ 30 から受信することとすると、この受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けている携帯電話ユーザ 1 から、そのコンテンツデータをコピーできることを可能としておけば、携帯電話ユーザ 1 にとっての利便性が向上する。

図 1 に示すように、携帯電話ユーザ 1 が受信したコンテンツデータを、コンテンツデータそのものおよび当該コンテンツデータを再生可能とするために必要な情報とともに、携帯電話ユーザ 2 に対してコピーさせる場合をコンテンツデータの「複製」と呼ぶ。

この場合に、携帯電話機 100 および 102 を介して、メモリカード 110 と 112 との間で暗号化されたコンテンツデータ（音楽データ）および再生のために必要な情報（再生情報）が複製される。ここで、「再生情報」とは、後に説明するように、所定の暗号化方式に従って暗号化されたコンテンツデータを復号可能なライセンスキーと、著作権保護にかかわる情報であるライセンス ID やアクセス再生に関する制限情報等とを有する。

このような構成とすることによって、一旦配信サーバ 30 より配信を受けたコンテンツデータについて受信者側での柔軟な利用が可能となる。

また、携帯電話機 100 および 102 が PHS（Personal Handy Phone）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、携帯電話ユーザ 1 と携帯電話ユーザ 2 との間における情報の複製を行なうことが可能である。

図 1 に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話ユーザ側で再生可能とするためにシステム上必要とされるのは、第 1 には、通信における暗号鍵を配信するための方式であり、さらに第 2 には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第 3 には、このように配信されたコンテンツデータの無断コピーを防止するための復号鍵保護を実現する構成である。

本発明の実施の形態においては、特に、配信、再生および複製の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェ

ック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびコンテンツ再生回路（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。また、再生回数の制限を設けた再生権の発行を可能とし、利用者にとって利便性が高く、かつ著作権に対して十分なセキュリティー強度を維持できる構成を説明する。

次に図 2 を用いて、図 1 に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する。

まず、配信サーバより配信されるデータについて説明する。Data は、音楽データ等のコンテンツデータである。コンテンツデータ Data には、ライセンスキー Kc で復号可能な暗号化が施される。ライセンスキー Kc によって復号可能な暗号化が施された暗号化コンテンツデータ {Data} Kc がこの形式で配信サーバ 30 より携帯電話ユーザに配布される。

なお、以下においては、{Y} X という表記は、データ Y を、復号鍵 X により復号可能な暗号化を施したデータであることを示すものとする。

さらに、配信サーバからは、暗号化コンテンツデータとともに、コンテンツデータに関するあるいはサーバへのアクセスに関する平文情報としての付加情報 Data-inf が配布される。また、ライセンスとしては、コンテンツデータ Data を識別するためのコードであるコンテンツ ID およびライセンスの発行を特定できる管理コードであるライセンス ID や、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件 AC に基づいて生成される、メモリのアクセスに対する制限に関する情報であるアクセス制限情報 AC 1 および再生回路における制御情報である再生回路制御情報 AC 2 等が存在する。

後ほど詳細に説明するが、再生回路制御情報 AC 2 は、再生回数の制限や複製（移動）可能なライセンス数を示す情報を含み、メモリカード内において情報の管理および更新が実行される。

図 3 には、図 1 に示したデータ配信システムにおいて使用されるキーデータ（鍵データ）等の特性が示される。

図 3 を参照して、コンテンツ再生回路（携帯電話機）およびメモリカードには

固有の公開暗号鍵 $KP_p(n)$ および $KP_{mc}(m)$ がそれぞれ設けられ、公開暗号鍵 $KP_p(n)$ および $KP_{mc}(m)$ はコンテンツ再生回路（携帯電話機）のクラス固有の秘密復号鍵 $K_p(n)$ およびメモ리카ードのクラス固有の秘密復号鍵 $K_{mc}(m)$ によってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機の種類ごとおよびメモ리카ードのクラスごとに異なる値を持つ。

また、メモ리카ードおよび再生回路のクラス証明書として、 $C_p(n)$ および $C_{mc}(m)$ がそれぞれ設けられる。ここで、自然数 m はメモ리카ードの、自然数 n はコンテンツ再生回路（携帯電話機）のクラスを区別するための番号を表わす。

これらのメモ리카ードおよびコンテンツ再生部固有の公開暗号鍵およびクラス証明書は、 $\{KP_{mc}(m) // C_{mc}(m)\}$ KP_{ma} および $\{KP_p(n) // C_p(n)\}$ KP_{ma} の形式で、出荷時にメモ리카ードおよび携帯電話機にそれぞれ記録される。後ほど詳細に説明するが、 KP_{ma} は配信システム全体で共通の認証鍵である。認証鍵 KP_{ma} を用いて認証データを復号すると、その復号結果から認証データの正当性が確認できる。言い換えれば、認証鍵 KP_{ma} は、クラス固有の公開暗号鍵およびその証明書であるクラス証明書を承認するために用いられる鍵である。なお、認証データを作成するための暗号化は、認証鍵と対をなす非対称な秘密鍵によって行なわれる。

メモ리카ード外とメモ리카ード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、再生および複製が行なわれるごとにサーバ30、携帯電話機100または102、メモ리카ード110または112において生成される共通鍵 $Ks_1 \sim Ks_4$ が用いられる。

ここで、共通鍵 $Ks_1 \sim Ks_4$ は、サーバ、携帯電話機もしくはメモ리카ード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵 $Ks_1 \sim Ks_4$ を「セッションキー」とも呼ぶこととする。

これらのセッションキー $Ks_1 \sim Ks_4$ は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモ리카ードによって管理される。具体的には、セッションキー Ks_1 は、配信サーバによって配信セッションごとに発生される。セッションキー Ks_2 は、メモ리카ードによって配信セッション

および複製（受信側）セッションごとに発生し、セッションキー $K_s 3$ は、同様にメモリカードにおいて再生セッションおよび複製（送信側）セッションごとに発生する。セッションキー $K_s 4$ は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

また、メモリカード100内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される暗号鍵 $KP_m(i)$ (i : 自然数) と、暗号鍵 $KP_m(i)$ で暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵 $K_m(i)$ が存在する。ここで、自然数 i は、各メモリカードを区別するための番号を表わす。

その他の鍵としては、再生回路に共通の秘密鍵として、主としてライセンスキー K_c の取得に利用される共通鍵方式における秘密鍵 K_{com} が存在する。秘密鍵 K_{com} は、配信サーバおよび携帯電話機の双方において保持され、ライセンスキー K_c 等の暗号化および取得のための復号処理にそれぞれ使用される。

なお、共通鍵 K_{com} を、公開鍵方式における公開暗号鍵 KP_{com} および秘密復号鍵 K_{com} の組に置き換えて運用することも可能である。この場合には、公開暗号鍵 KP_{com} は配信サーバに保持されてライセンスキー K_c の暗号化に使用され、秘密復号鍵 K_{com} は、携帯電話機に保持されてライセンスキー K_c の取得に使用される。

図4を参照して、ライセンスサーバ10は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンス ID 等の配信情報を保持するための情報データベース304と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、情報データベース304および課金データベース302からのデータをデータバス BS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

データ処理部 310 は、データバス BS1 上のデータに応じて、データ処理部 310 の動作を制御するための配信制御部 315 と、配信制御部 315 に制御されて、配信セッション時にセッションキー K_s1 を発生するためのセッションキー発生部 316 と、メモリカードおよび携帯電話機から送られてきた認証のための
5 認証データ $\{K_{Pmc}(m) // C_{mc}(m)\}$ K_{Pma} および $\{K_{Pp}(n) // C_p(n)\}$ K_{Pma} を通信装置 350 およびデータバス BS1 を介して受けて、認証鍵 K_{Pma} による復号処理を行なう復号処理部 312 とを含む。

データ処理部 310 は、さらに、セッションキー発生部 316 より生成されたセッションキー K_s1 を復号処理部 312 によって得られた公開暗号鍵 $K_{Pmc}(m)$
10 を用いて暗号化して、データバス BS1 に出力するための暗号化処理部 318 と、セッションキー K_s1 によって暗号化された上で送信されたデータをデータバス BS1 をより受けて、復号処理を行なう復号処理部 320 と、再生回路に共通な秘密鍵 K_{com} を保持する K_{com} 保持部 322 とを含む。

データ処理部 310 は、さらに、配信制御部 315 から与えられるライセンス
15 キー K_c および再生回路制御情報 AC2 を再生回路共通の秘密鍵 K_{com} で暗号化する暗号化処理部 324 と、暗号化処理部 324 から出力されたデータを復号処理部 320 によって得られたメモリカード固有の公開暗号鍵 $K_{Pm}(i)$ によって暗号化するための暗号化処理部 326 と、暗号化処理部 326 の出力を、復号処理部 320 から与えられるセッションキー K_s2 によってさらに暗号化してデータバス
20 BS1 に出力するための暗号化処理部 328 とを含む。

なお、共通鍵方式における秘密復号 K_{com} に代えて、公開鍵方式における公開暗号鍵 K_{Pcom} および秘密復号鍵 K_{com} の組を用いる場合には、 K_{com} 保持部 322 に相当する部分に公開暗号鍵 K_{Pcom} が保持される。さらに、暗号化処理部 324 によって、公開暗号鍵 K_{Pcom} による暗号化が行なわれる。

25 ライセンスサーバ 10 の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図 5 を参照して、携帯電話機 100 においては、携帯電話機のクラスを表わす自然数 $n = 1$ 、携帯電話機を個別に識別する自然数 $i = 1$ とする。

携帯電話機 100 は、携帯電話網により無線伝送される信号を受信するための

アンテナ 1102 と、アンテナ 1102 からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ 1102 に与えるための送受信部 1104 と、携帯電話機 100 の各部のデータ授受を行なうためのデータバス BS2 と、データバス BS2 を介して携帯電話機 100 の動作を制御するためのコントローラ 1106 とを含む。

携帯電話機 100 は、さらに、外部からの指示を携帯電話機 100 に与えるためのタッチキー部 1108 と、コントローラ 1106 等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ 1110 と、通常の通話動作において、データバス BS2 を介して与えられる受信データに基づいて音声再生するための音声再生部 1112 と、外部との間でデータの授受を行なうためのコネクタ 1120 と、コネクタ 1120 からのデータをデータバス BS2 に与え得る信号に変換し、または、データバス BS2 からのデータをコネクタ 1120 に与え得る信号に変換するための外部インタフェース部 1122 とを含む。

携帯電話機 100 は、さらに、配信サーバ 30 からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード 110 と、メモリカード 110 とデータバス BS2 との間のデータの授受を制御するためのメモリインタフェース 1200 と、携帯電話機のクラスごとにそれぞれ設定される公開暗号鍵 K_P(1) およびクラス証明書 C_p(1) を公開復号鍵 K_P_a で復号可能な状態に暗号化したデータを保持する認証データ保持部 1500 を含む。

携帯電話機 100 は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵である K_p(1) を保持する K_p 保持部 1502 と、データバス BS2 から受けたデータを K_p(1) によって復号しメモリカードによって発生されたセッションキー K_s3 を得る復号処理部 1504 と、メモリカード 110 に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード 110 との間でデータバス BS2 上においてやり取りされるデータを暗号化するためのセッションキー K_s4 を乱数等により発生するセッションキー発生部 1508 と、生成されたセッションキー K_s4 を復号処理部 1504 によって得られたセッションキー K_s3 によって暗号化しデータバス BS2 に出力する暗号化処理部 1506 と、デー

タバス BS 2 上のデータをセッションキー Ks 4 によって復号して出力する復号処理部 1 5 1 0 とを含む。

携帯電話機 1 0 0 は、さらに、再生回路に共通に設定される秘密鍵 Kcom を保持する Kcom 保持部 1 5 1 2 と、復号処理部 1 5 1 0 が出力する {Kc//AC 2} Kcom を秘密鍵 Kcom で復号しライセンスキー Kc および再生回路制御情報 AC 2 を出力する復号処理部 1 5 1 4 と、データバス BS 2 より暗号化コンテンツデータ {Data} Kc を受けて、復号処理部 1 5 1 4 より取得してライセンスキー Kc によって復号しコンテンツデータを出力する復号処理部 1 5 1 6 とを含む。携帯電話機 1 0 0 は、さらに、復号処理部 1 5 1 6 の出力を受けてコンテンツデータを再生するための音楽再生部 1 5 1 8 と、音楽再生部 1 5 1 8 と音声再生部 1 1 1 2 の出力を受けて、動作モードに応じて選択的に出力するための切換部 1 5 2 5 と、切換部 1 5 2 5 の出力を受けて、ヘッドホン 1 3 0 と接続するための接続端子 1 5 3 0 とを含む。

なお、共通鍵 Kcom に代えて公開鍵方式における公開暗号鍵 KPcom および秘密復号鍵 Kcom の組を用いる場合には、Kcom 保持部 1 5 1 2 に相当する部分に秘密復号鍵 Kcom が保持される。さらに、復号処理部 1 5 1 4 によって、秘密復号鍵 Kcom による復号が行なわれる。

また、図 5 においては、説明の簡素化のため、携帯電話機のうち本発明のコンテンツデータの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては一部割愛している。

図 5 に記載されたブロックのうち、アンテナ 1 1 0 2、送受信部 1 1 0 4、コントローラ 1 1 0 6、キー 1 1 0 8、ディスプレイ 1 1 1 0、音声再生部 1 1 1 2、コネクタ 1 1 2 0、外部インタフェース 1 1 2 2、切換部 1 5 2 5 および接続端子 1 5 3 0 の、通話処理に関するあるいは通話処理と共用されるブロック群除いた部分が、コンテンツデータの配信および再生に関するコンテンツ再生部に相当する。なお、携帯電話ユーザの利便性を図るために、携帯電話機 1 0 0 のうちのコンテンツ再生部に相当するブロック群を、音楽再生モジュールとして着脱可能なモジュール化する構成を採用することも可能である。

携帯電話機 1 0 0 の各構成部分の各セッションにおける動作については、後ほ

どフローチャートを使用して詳細に説明する。

図6を参照して、既に説明したように、公開暗号鍵 $KP_m(i)$ およびこれに対応する秘密復号鍵 $K_m(i)$ は、メモ리카ードごとに固有の値であるが、メモ리카ード110においては、この自然数 $i=1$ として取扱う。また、メモ리카ードの固有の公開暗号鍵および秘密復号鍵として、 $KP_{mc}(m)$ および $K_{mc}(m)$ が設けられ、メモ리카ードのクラス証明書として $C_{mc}(m)$ が設けられるが、メモ리카ード110においては、これらは自然数 $m=1$ でそれぞれ表わされるものとする。

メモ리카ード110は、認証データ $\{KP_{mc}(1) // C_{mc}(1)\}$ KP_{ma} を保持する認証データ保持部1400と、メモ리카ードの種類ごとに設定される固有の復号鍵である $K_{mc}(1)$ を保持する K_{mc} 保持部1402と、メモ리카ードごとに固有に設定される秘密復号鍵 $K_m(1)$ を保持する $K_m(1)$ 保持部1421と、 $K_m(1)$ によって復号可能な公開暗号鍵 $KP_m(1)$ を保持する $KP_m(1)$ 保持部1416とを含む。認証データ保持部1400は、メモ리카ード110に対応して設定される公開暗号鍵 $KP_{mc}(1)$ を認証鍵 KP_{ma} で復号することで認証可能な状態に暗号化して保持する。

このように、メモ리카ードという記録装置の公開暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンスキーの管理をメモ리카ード単位で実行することが可能になる。

メモ리카ード110は、さらに、メモリインタフェース1200との間で信号を端子1202を介して授受するデータバスBS3と、データバスBS3にメモリインタフェース1200から与えられるデータから、メモ리카ードの種類ごとに固有の秘密復号鍵 $K_{mc}(1)$ を $K_{mc}(1)$ 保持部1402から受けて配信サーバ30が配信セッションにおいて生成したセッションキー K_{s1} 、または他のメモ리카ードが複製セッションにおいて生成したセッションキー K_{s3} を接点 Pa に出力する復号処理部1404とを含む。

メモ리카ード110は、さらに、 KP_{ma} 保持部1414から認証鍵 KP_{ma} を受けて、データバスBS3に与えられるデータから認証鍵 KP_{ma} による復号処理を実行して復号結果を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1444

によって選択的に与えられるデータを暗号化してデータバス BS 3 に出力する暗号化処理部 1 4 0 6 とを含む。

メモリカード 1 1 0 は、さらに、配信、再生および複製の各セッションにおいてセッションキーを発生するセッションキー発生部 1 4 1 8 と、セッションキー発生部 1 4 1 8 の出力したセッションキー $K_s 3$ を復号処理部 1 4 0 8 によって得られる公開暗号鍵 $KP_p (n)$ もしくは $KP_{mc} (m)$ によって暗号化してデータバス BS 3 に送出する暗号化処理部 1 4 1 0 と、BS 3 よりセッションキー $K_s 3$ によって暗号化されたデータを受けてセッションキー発生部 1 4 1 8 より得たセッションキー $K_s 3$ によって復号し、復号結果をデータバス BS 4 に送出する復号処理部 1 4 1 2 とを含む。

メモリカード 1 1 0 は、さらに、「複製」時にデータバス BS 4 上のデータを他のメモリカードの公開暗号鍵 $KP_m (i)$ ($i \neq 1$) で暗号化する暗号化処理部 1 4 2 4 と、データバス BS 4 上のデータを公開暗号鍵 $KP_m (1)$ と対をなすメモリカード 1 1 0 固有の秘密復号鍵 $K_m (1)$ によって復号するための復号処理部 1 4 2 2 と、公開暗号鍵 $KP_m (1)$ で暗号化されている、ライセンスキー K_c および再生回路制御情報 AC 2 をデータバス BS 4 より受けて格納するとともに、暗号化コンテンツデータ {Data} K_c および付加情報 Data-inf をデータバス BS 3 より受けて格納するためのメモリ 1 4 1 5 とを含む。

メモリカード 1 1 0 は、さらに、復号処理部 1 4 2 2 によって得られるライセンス ID、コンテンツ ID およびアクセス制限情報 AC 1 を保持するためのライセンス情報保持部 1 4 4 0 と、データバス BS 3 を介して外部との間でデータ授受を行ない、データバス BS 4 との間で再生情報等を受けて、メモリカード 1 1 0 の動作を制御するためのコントローラ 1 4 2 0 とを含む。ライセンス情報保持部 1 4 4 0 は、データバス BS 4 との間でライセンス ID、コンテンツ ID およびアクセス制限情報 AC 1 のデータの授受が可能である。

図 7 を参照して、ライセンス情報保持部 1 4 4 0 は、 N 個 (N : 自然数) のバンクを有し、各ライセンスに対応するライセンス情報である、ライセンス ID、データコンテンツ ID データおよびアクセス制限情報 AC 1 をバンクごとに保持する。

図 8 を参照して、アクセス制限情報 AC 1 は、再生回数制限情報 Sub_Play と、所有ライセンス数 Sub_Move とを含む。図 8 においては、再生回数制限情報 Sub_Play は、一例として 8 ビットのデータである。Sub_Play の値が FF(h) である場合には再生回数に制限がないことを示し、その値が 0 (h) である場合には、
5 もはや再生不能であることを示す。また、Sub_Play の値が 1(h) ~ 7F(h) の範囲である場合は、この値は再生可能な回数を示し、再生されるごとに Sub_Play の値は減じられる。なお、(h) は、16 進数表示を意味する。

また、図 8 においては、所有ライセンス数 Sub_Move は、一例として同様に 8 ビットのデータで示される。Sub_Move の値が FF(h) である場合には、複製が禁止
10 されていることを示す。また、Sub_Move の値が 0 (h) ~ 7F(h) の範囲である場合は、この値は所有ライセンス数を示し、他のメモ리카ードに複製させるごとに、複製したライセンス数に応じて Sub_Move の値は減じられ、その値が 0 (h) となった場合には、もはや複製するライセンスが無いことを示す。

アクセス制限情報 AC 1 は、ライセンス購入時に利用者側からの指定に応じて生成されるライセンス購入条件 AC に応じて、配信動作時に配信サーバ 30 によって発行され、再生および複製動作が実行されるごとに、メモ리카ード 110 内
15 において、更新および保持される。

なお、図 6 において、実線で囲んだ領域は、メモ리카ード 110 内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能
20 化するためのモジュール TRM に組込まれているものとする。このようなモジュールは、一般には、内部解析や改ざんを物理的および論理的に防衛する技術を用いた、外部から直接アクセス不可能なタンパーレジスタントモジュール (Tamper Resistant Module) である。

もちろん、メモリ 1415 も含めて、モジュール TRM 内に組込まれる構成としてもよい。しかしながら、図 6 に示したような構成とすることで、メモリ 1415 中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ 1415 中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタントモジュール内にメモリ
25

1 4 1 5 を設ける必要がないので、製造コストが低減されるという利点がある。

次に、本発明の実施の形態に従うデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

まず、図 9 および図 10 のフローチャートを用いて、実施の形態 1 に従うデータ配信システムにおけるコンテンツの購入時に発生する配信セッション時の動作
5 (以下、配信動作ともいう) を説明する。

図 9 および図 10 においては、携帯電話ユーザ 1 が、メモリカード 110 を用いることで、携帯電話機 100 を介して配信サーバ 30 から音楽データであるコンテンツデータの配信を受ける場合の動作が説明される。

10 図 9 を参照して、まず、携帯電話ユーザ 1 の携帯電話機 100 から携帯電話ユーザによりタッチキー部 1108 のキーボタンの操作等によって、配信リクエストがなされる (ステップ S100)。

メモリカード 110 においては、この配信リクエストに応じて、認証データ保持部 1400 より認証データ {KPmc (1) //Cmc (1)} KPma が出力される (ステップ S102)。
15

携帯電話機 100 は、メモリカード 110 から受理した認証のための認証データ {KPmc (1) //Cmc (1)} KPma に加えて、コンテンツ再生回路の認証のための認証データ {KPP (1) //Cp (1)} KPma と、コンテンツ ID、ライセンス購入条件データ AC とを配信サーバ 30 に対して送信する (ステップ S104)。

20 配信サーバ 30 では、携帯電話機 100 からコンテンツ ID、認証データ {KPP (1) //Cp (1)} KPma、{KPmc (1) //Cmc (1)} KPma、{KPP (1) //Cp (1)} KPma、ライセンス購入条件 AC を受信し (ステップ S106)、復号処理部 312 において認証鍵 KPma で復号処理を実行して、メモリカード 110 の公開暗号鍵およびクラス証明書である KPmc (1) および Cmc (1) と、携帯電話
25 機 100 のコンテンツ再生回路の公開暗号鍵およびクラス証明書である KPP (1) および Cp (1) を受理する (ステップ S108)。

配信制御部 315 は、受理したクラス証明データ Cmc (1) および Cp (1) に基づいて、認証サーバ 12 に対して照会を行ない、これらのクラス証明書が有効であれば正規の機器であり、これらの公開暗号鍵が有効であることが確認される。

公開暗号鍵が有効である場合には次の処理（ステップ S 1 1 2）に移行し、これらの公開暗号鍵が無効である場合には、処理を終了（ステップ S 1 6 0）する（ステップ S 1 1 0）。

- 5 なお、認証データ {KPmc (1)} KPma および認証データ {KPp (1)} KPma は、それぞれが認証鍵 KPma によって復号することで、その正当性が判断可能な暗号化が施されているため、認証サーバ 12 に対して照会を行わず、ライセンスサーバ 10 の配信制御部 315 が、認証鍵 KPma による復号結果から独自に認証を行なう構成とすることもできる。

- 10 照会の結果、正規のクラス証明書を持つメモリカードと再生回路とを備える携帯電話機からのアクセスであることが確認されると、配信サーバ 30 において、セッションキー発生部 316 は、配信のためのセッションキー Ks1 を生成する。セッションキー Ks1 は、復号処理部 312 によって得られたメモリカード 110 に対応する公開暗号鍵 KPmc (1) によって、暗号化処理部 318 によって暗号化される（ステップ S 1 1 2）。

- 15 暗号化されたセッションキー Ks1 は、{Ks1} Kmc (1) として、データベース BS1 および通信装置 350 を介して外部に出力される（ステップ S 1 1 4）。

- 20 携帯電話機 100 が、暗号化されたセッションキー {Ks1} Kmc (1) を受信すると（ステップ S 1 1 6）、メモリカード 110 においては、メモリインタフェース 1200 を介して、データベース BS3 に与えられた受信データを、復号処理部 1404 が、保持部 1402 に保持されるメモリカード 110 固有の秘密復号鍵 Kmc (1) により復号処理することにより、セッションキー Ks1 を復号し抽出する（ステップ S 1 1 8）。

- 25 コントローラ 1420 は、配信サーバ 30 で生成されたセッションキー Ks1 の受理を確認すると、セッションキー発生部 1418 に対して、メモリカードにおいて配信動作時に生成されるセッションキー Ks2 の生成を指示する。

暗号化処理部 1406 は、切換スイッチ 1442 の接点 Pa を介して復号処理部 1404 より与えられるセッションキー Ks1 によって、切換スイッチ 1444 および 1446 の接点を順次切換えることによって与えられるセッションキー Ks2 および公開暗号鍵 KPm (1) を 1 つのデータ列として暗号化して、{Ks2

./Kp_m(1) } K_s1 をデータバス BS 3 に出力する (ステップ S 1 2 0)。

データベース BS 3 に出力された暗号データ {K_s2//Kp_m(1) } K_s1 は、データベース BS 3 から端子 1 2 0 2 およびメモリーインタフェース 1 2 0 0 を介して携帯電話機 1 0 0 に送信され、携帯電話機 1 0 0 から配信サーバ 3 0 に送信される
5 (ステップ S 1 2 2)。

配信サーバ 3 0 は、暗号化データ {K_s2//Kp_m(1) } K_s1 を受信して、復号処理部 3 2 0 においてセッションキー K_s1 による復号処理を実行し、メモリーカード 1 1 0 で生成されたセッションキー K_s2 およびメモリーカード 1 1 0 固有の公開暗号鍵 Kp_m(1) を受領する (ステップ S 1 2 4)。

10 配信制御部 3 1 5 は、ステップ S 1 0 6 で取得したコンテンツ ID およびライセンス購入条件 AC に従って、ライセンス ID、アクセス制限情報 AC 1 および再生回路制御情報 AC 2 を生成する (ステップ S 1 2 6)。さらに、暗号化コンテンツデータを復号するためのライセンスキー K_c を情報データベース 3 0 4 より取得する (ステップ S 1 2 8)。

15 図 1 0 を参照して、配信制御部 3 1 5 は、取得したライセンスキー K_c および再生回路制御情報 AC 2 を暗号化処理部 3 2 4 に与える。暗号化処理部 3 2 4 は、Kcom 保持部 3 2 2 より得られる、再生回路共通の秘密鍵 Kcom によって、ライセンスキー K_c および再生回路制御情報 AC 2 を暗号化する (ステップ S 1 3 0)。

暗号化処理部 3 2 4 が出力する暗号化データ {K_c//AC 2} Kcom と、配信制御
20 部 3 1 5 が出力するライセンス ID、コンテンツ ID およびアクセス制限情報 AC 1 とは、暗号化処理部 3 2 6 によって、復号処理部 3 2 0 によって得られたメモリーカード 1 1 0 固有の公開暗号鍵 Kp_m(1) によって暗号化される (ステップ S 1 3 2)。暗号化処理部 3 2 8 は、暗号化処理部 3 2 6 の出力を受けて、メモリーカード 1 1 0 において生成されたセッションキー K_s2 によって暗号化する。暗号化
25 処理部 3 2 8 より出力された暗号化データは、データベース BS 1 および通信装置 3 5 0 を介して携帯電話機 1 0 0 に送信される (ステップ S 1 3 4)。

このように、配信サーバおよびメモリーカードでそれぞれ生成される暗号鍵をやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信において

も事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

携帯電話機 100 は、送信された暗号化データ { { {Kc//AC 2} Kcom//ライセンス ID//コンテンツ ID// AC 1} Km (1) } Ks2 を受信し (ステップ S 136)、
5 メモリカード 110 においては、メモリインタフェース 1200 を介して、データベース BS3 に与えられた受信データを復号化処理部 1412 によって復号する。復号処理部 1412 は、セッションキー発生部 1418 から与えられたセッションキー Ks2 を用いてデータベース BS3 の受信データを復号しデータベース BS4 に出力する (ステップ S 138)。

10 この段階で、データベース BS4 には、Km (1) 保持部 1421 に保持される秘密復号鍵 Km (1) で復号可能な { {Kc//AC 2} Kcom //ライセンス ID//コンテンツ ID//AC 1} Km (1) が出力される。コントローラ 1420 の指示によって、{ {Kc//AC 2} Kcom//ライセンス ID//コンテンツ ID//AC 1} Km (1) は、メモリ 1415 に記録される (ステップ S 140)。一方、{ {Kc//AC 2} Kcom//ラ
15 イセンス ID//コンテンツ ID//AC 1} Km (1) は、復号処理部 1422 において、秘密復号鍵 Km (1) によって復号され、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC1 のみが受理される (ステップ S 142)。

ライセンス ID、コンテンツ ID およびアクセス制限情報 AC1 については、ライセンス情報保持部 1440 に記録される (ステップ S 144)。

20 ステップ S 144 までの処理がメモリ回路で正常に終了した段階で、携帯電話機 100 から配信サーバ 30 にコンテンツデータの配信要求がなされる (ステップ S 146)。

配信サーバ 30 は、コンテンツデータの配信要求を受けて、情報データベース 304 より、暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf を取得して、これらのデータをデータベース BS1 および通信装置 350 を介して出力する (ステップ S 148)。

携帯電話機 100 は、{Data} Kc//Data-inf を受信して、暗号化コンテンツデータ {Data} Kc および Data-inf を受理する (ステップ S 150)。暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf はメモリインタフェース 1

200および端子1202を介してメモリカード110のデータバスBS3に伝達される。メモリカード110においては、受信した{Data}Kcおよび付加情報Data-infがそのままメモリ1415に記録される(ステップS152)。

さらに、メモリカード110から配信サーバ30へは、配信受理の通知が送信され(ステップS154)、配信サーバ30で配信受理を受信すると(ステップS156)、課金データベース302への課金データの格納等を伴って、配信終了の処理が実行され(ステップS158)、全体の処理が終了する(ステップS160)。

このようにして、携帯電話機100のコンテンツ再生部およびメモリカード110が正規の機器であること、同時に、それぞれがクラス証明書Cp(1)およびCmc(1)とともに暗号化して送信できた公開暗号鍵Kp(1)およびKmc(1)が有効であることを確認した上で、コンテンツデータを配信することができ、十分なセキュリティ強度を確保することができる。

次に、図11のフローチャートを用いて、携帯電話機100内において、メモリカード110に保持された暗号化コンテンツデータから音楽を再生し、外部に出力するための再生セッション時の動作(以下、再生動作ともいう)を説明する。

図11を参照して、携帯電話機100のタッチキー部1108等からの携帯電話ユーザ1の指示により、再生リクエストが生成される(ステップS200)。携帯電話機100は、再生リクエストの生成に応じて、認証データ保持部1500より、認証鍵KPmaで復号することで認証可能な認証データ{KPp(1)//Cp(1)}KPmaをデータバスBS2に出力する(ステップS202)。

認証データ{KPp(1)//Cp(1)}KPmaは、データバスBS2およびメモリインタフェース1200を介してメモリカード110に伝達される。

メモリカード110においては、端子1202を介してデータバスBS3に伝達される認証のための暗号化データ{KPp(1)//Cp(1)}KPmaは、復号処理部1408に取込まれる。復号処理部1408は、KPma保持部1414から認証鍵KPmaを受けて、データバスBS3のデータを復号処理し、コンテンツ再生部すなわち携帯電話機100の種類に固有の公開暗号鍵KPp(1)およびクラス証明書Cp(1)を得る。コントローラ1420は、データバスBS3を介して公開

暗号鍵 $K_{Pp}(1)$ およびクラス証明書 $C_p(1)$ を受理する（ステップ S 2 0 4）。

コントローラ 1 4 2 0 は、復号処理部 1 4 0 8 の復号結果に基づいて、受理した携帯電話機 1 0 0 のコンテンツ再生回路の認証作業を行ない、携帯電話機 1 0 0 のコンテンツ再生回路が承認されたものである場合には処理を次のステップ（ステップ S 2 0 8）に進める（ステップ S 2 0 6）。一方、携帯電話機 1 0 0 のコンテンツ再生回路が非承認である場合には、再生セッションの処理を終了する（ステップ S 2 4 0）。

次に、コントローラ 1 4 2 0 は、セッションキー発生部 1 4 1 8 に、再生セッションにおけるセッションキー $K_s 3$ の生成をデータバス BS 4 を介して指示する。セッションキー発生部 1 4 1 8 によって生成されたセッションキー $K_s 3$ は、暗号化処理部 1 4 1 0 に送られる。暗号化処理部 1 4 1 0 は、復号処理部 1 4 0 8 によって得られた携帯電話機 1 0 0 の公開暗号鍵 $K_{Pp}(1)$ によってセッションキー $K_s 3$ を暗号化し $K_{Pp}(1)$ に対応する秘密復号鍵 $K_p(1)$ で復号可能な暗号化データ $\{K_s 3\} K_p(1)$ をデータバス BS 3 に出力する（ステップ S 2 0 8）。

携帯電話機 1 0 0 は、端子 1 2 0 2 およびメモリインタフェース 1 2 0 0 を介して、データバス BS に暗号化データ $\{K_s 3\} K_p(1)$ を受ける。暗号化データ $\{K_s 3\} K_p(1)$ は、復号処理部 1 5 0 4 によって復号され、メモ리카ード 1 1 0 で生成されたセッションキー $K_s 3$ が受理される（ステップ S 2 1 0）。

コントローラ 1 1 0 6 は、セッションキー $K_s 3$ の受理に応じて、セッションキー発生部 1 5 0 8 に対して、再生セッションにおいて携帯電話機 1 0 0 で生成されるセッションキー $K_s 4$ の発生をデータバス BS 2 を介して指示する。生成されたセッションキー $K_s 4$ は暗号化処理部 1 5 0 6 に送られ、復号処理部 1 5 0 4 によって得られたセッションキー $K_s 3$ によって暗号化された $\{K_s 4\} K_s 3$ がデータバス BS 2 に受理される（ステップ S 2 1 2）。

暗号化されたセッションキー $\{K_s 4\} K_s 3$ は、メモリインタフェース 1 2 0 0 を介してメモ리카ード 1 1 0 に伝達される。メモ리카ード 1 1 0 においては、データバス BS 3 に伝達される暗号化されたセッションキー $\{K_s 4\} K_s 3$ を復号処理部 1 4 1 2 によって復号し、携帯電話機 1 0 0 で生成されたセッションキー $K_s 4$ を受理する（ステップ S 2 1 4）。

セッションキーKs 4の受理に応じて、コントローラ1 4 2 0は、ライセンス情報保持部1 4 4 0内の対応するアクセス制限情報AC 1を確認する。

5 コントローラ1 4 2 0は、まず所有ライセンス数 Sub_Move を確認し、この値が0であるときは、すでにライセンスが無い状態であるので再生セッションを終了する（ステップS 2 4 0）。一方、所有ライセンス数 Sub_Move の値が0以外であるときには、処理を次のステップに進める（ステップS 2 1 6）。

10 次のステップにおいては、コントローラ1 4 2 0は、再生回数制限情報 Sub_Play を確認し、この値が0であるときは、すでに再生不能の状態であるので再生セッションを終了する（ステップS 2 4 0）。再生回数制限情報 Sub_Play の値が1 (h)～7F(h)である場合には、Sub_Play の値すなわち再生可能回数を1減じて（ステップS 2 2 0）、再生セッションの処理を進める。一方、再生回数制限情報 Sub_Play の値がFF(h)である場合には、当該ライセンスについては再生回数の制限がないことを意味するので、ステップS 2 2 0を実行することなく再生セッションの処理が実行される（ステップS 2 1 8）。

15 ステップS 2 1 8において、当該再生セッションにおいて再生が可能であると判断された場合には、メモリに記録された再生リクエスト曲のライセンスキーKc および再生回路制御情報 AC 2の復号処理が実行される。具体的には、コントローラ1 4 2 0の指示に応じて、メモリ1 4 1 5からデータバス BS 4に読出された暗号化データ { {Kc//AC 2} Kcom//ライセンス ID//コンテンツ ID//AC 1} Km
20 (1)を復号処理部1 4 2 2がメモリカード1 1 0固有の秘密復号鍵 Km (1)によって復号し、共通の秘密鍵 Kcom によって復号可能な暗号化データ {Kc//AC 2} Kcom がデータバス BS 4上に得られる（ステップS 2 2 2）。

25 得られた暗号化データ {Kc// AC 2} Kcom は、切換スイッチ1 4 4 4の接点Pdを介して暗号化処理部1 4 0 6に送られる。暗号化処理部1 4 0 6は、切換スイッチ1 4 4 2の接点 Pb を介して復号処理部1 4 1 2より受けたセッションキー Ks 4によってデータバス BS 4から受けた暗号化データをさらに暗号化し、
{ {Kc//AC 2} Kcom} Ks 4をデータバス BS 3に出力する（ステップS 2 2 4）。

データバス BS 3に出力された暗号化データは、メモリインタフェース1 2 0 0を介して携帯電話機1 0 0に送出される。

携帯電話機 100 においては、メモリインタフェース 1200 を介してデータベース BS2 に伝達される暗号化データ { {Kc//AC2} Kcom} Ks4 を復号処理部 1510 によって復号処理を行ない、暗号化されたライセンスキー Kc および再生回路制御情報 AC2 を受取する (ステップ S226)。

- 5 復号処理部 1514 は、暗号化データ {Kc//AC2} Kcom を、Kcom 保持部 1512 から受けた再生回路に共通の秘密鍵 Kcom によって復号し、ライセンスキー Kc および再生回路制御情報 AC2 を受取する (ステップ S228)。復号処理部 1514 は、ライセンスキー Kc を復号処理部 1516 に伝達し、再生回路制御情報 AC2 をデータベース BS2 に出力する。

- 10 コントローラ 1106 は、データベース BS2 を介して、再生回路制御情報 AC2 を受取して再生の可否の確認を行なう (ステップ S230)。

- ステップ S230 においては、再生回路制御情報 AC2 によって再生不可と判断される場合には、再生セッションは終了される (ステップ S240)。一方、再生可能である場合には、メモリカード 110 よりメモリに記録されたリクエスト曲の暗号化されたコンテンツデータ {Data} Kc がデータベース BS3 に出力され、メモリインタフェース 1200 を介して携帯電話機 100 に伝達される (ステップ S232)。

- 携帯電話機 100 においては、メモリカード 210 から出力されデータベース BS2 に伝達された暗号化コンテンツデータ {Data} Kc を復号処理部 1516 においてライセンスキー Kc によって復号し、平文化されたコンテンツデータ Data を得ることができる (ステップ S234)。復号された平文化コンテンツデータ Data は音楽再生部 1518 によって音楽信号に変換され (ステップ S236)、混合部 1525 および端子 1530 を介して外部に再生された音楽を出力することによって処理が終了する (ステップ S240)。

- 25 このような構成とすることで、メモリカード 110 側において、コンテンツ再生回路である携帯電話機 100 の認証を行なった上で、再生処理を禁止することが可能となる。また、メモリカード内で更新、保持されるアクセス制限情報を反映した再生動作を実行することができる。

再生セッションにおいても、携帯電話機 100 およびメモリカード 110 でそ

それぞれ生成される暗号鍵をやりとりし、お互いが受領した暗号鍵を用いた暗号化
を実行して、その暗号化データを相手方に送信する。この結果、配信セッション
と同様に、再生セッションにおいてもデータのそれぞれの送受信においても事実
上の相互認証を行なうことができ、データ配信システムのセキュリティーを向上
5 させることができる。

次に、図 1 2、図 1 3 および図 1 4 のフローチャートを用いて、2つのメモリ
カード間におけるコンテンツデータの複製セッション時の動作（以下、複製動作
とも称する）を説明する。

図 1 2、図 1 3 および図 1 4 においては、2つのメモリカード 1 1 0 および 1
1 2 の間で携帯電話機 1 0 0 および 1 0 2 を介した、コンテンツデータおよびキ
ーデータ等の複製動作が説明される。

図 1 2、図 1 3 および図 1 4 においては、携帯電話機 1 0 0 およびメモリカー
ド 1 1 0 についての種類を識別するための自然数を $m=1$ および $n=1$ とし、携
帯電話機 1 0 2 およびメモリカード 1 1 2 についての種類を識別するため自然数
15 を $m=2$ および $n=2$ とする。また、メモリカード 1 1 0 および 1 1 2 を識別す
るための自然数 i は、それぞれ $i=1$ および $i=2$ であるものとする。

携帯電話機 1 0 0 およびメモリカード 1 1 0 が送信側であり、携帯電話機 1 0
2 およびメモリカード 1 1 2 が受信側であるものとする。また、携帯電話機 1 0
2 も、メモリカード 1 1 0 と同様の構成を有するメモリカード 1 1 2 が装着され
20 ているものとする。以下、メモリカード 1 1 2 の各構成部分については、メモリ
カード 1 1 0 の対応する部分と同一の符号を用いて説明する。

図 1 2 を参照して、まず、送信側である携帯電話ユーザ 1 の携帯電話機 1 0 0
から、携帯電話ユーザ 1 によりタッチキー部 1 1 0 8 のキーボタンの操作等によ
って、コンテンツ複製リクエストがなされる。（ステップ S 3 0 0）。

25 生成された複製リクエストは、受信側である携帯電話ユーザ 2 の携帯電話機 1
0 2 を介してメモリカード 1 1 2 に伝達される。メモリカード 1 1 2 においては、
認証データ保持部 1 5 0 0 より、メモリカード 1 1 2 に対応する公開暗号鍵 $KP_{mc}(2)$
およびクラス証明書 $C_{mc}(2)$ が暗号化された認証データ $\{KP_{mc}(2)$
 $//C_{mc}(2)\}$ KP_{ma} が出力される（ステップ S 3 0 2）。

メモ리카ード 1 1 2 の認証データ {KPmc (2) //Cmc (2)} KPma は、携帯電話ユーザ 2 の携帯電話機 1 0 2 から送信され、携帯電話ユーザ 1 の携帯電話機 1 0 0 を経由してメモ리카ード 1 1 0 に受信される (ステップ S 3 0 4)。

5 メモ리카ード 1 1 0 においては、復号処理部 1 4 0 8 によって、メモ리카ード 1 1 2 の認証データが復号され、メモ리카ード 1 1 2 に関するクラス証明書 Cmc (2) および公開暗号鍵 KPmc (2) が受理される (ステップ S 3 0 6)。コントローラ 1 4 2 0 は、データベース BS 3 を介して復号処理部 1 4 0 8 の復号結果に基づいて、認証作業を実行する (ステップ S 3 0 8)。

10 コントローラ 1 4 2 0 は、メモ리카ード 1 1 2 に関する認証データ {KPmc (2) //Cmc (2)} KPma を認証鍵 KPma にて復号した復号結果から、認証データ {KPmc (2) //Cmc (2)} KPma が正規のキーから出力された認証データであることを確認することができる。この確認を実行し、正規のキーから出力された有効な認証データである場合には、公開暗号鍵 KPmc (2) およびクラス証明書 Cmc (2) を承認して、次のステップ S 3 1 0 を実行する。一方、正規のキーから出力されたことが確認できない無効な認証データである場合においては、複製セッションを終了する (ステップ S 3 7 0)。

20 この場合においては、コントローラ 1 4 2 0 は、セッションキー発生部 1 4 1 8 に対して、複製セッション時に送信側で発生されるセッションキー Ks 3 の出力を指示する。セッションキー発生部 1 4 1 8 によって生成されたセッションキー Ks 3 は、暗号化処理部 1 4 1 0 に伝達される。

25 暗号化処理部 1 4 1 0 は、さらに、ステップ S 3 0 6 において復号処理部 1 4 0 8 によって復号されたメモ리카ード 1 1 2 の公開暗号鍵 KPmc (2) を受けて、KPmc (2) によってセッションキー Ks 3 を暗号化する。これにより、暗号化されたセッションキー {Ks 3} Kmc (2) がデータベース BS 3 に出力される (ステップ S 3 1 2)。データベース BS 3 に出力された {Ks 3} Kmc (2) は、携帯電話機 1 0 0 および携帯電話機 1 0 2 を介してメモ리카ード 1 1 2 に伝達される。

メモ리카ード 1 1 2 は、メモ리카ード 1 1 0 から出力された {Ks 3} Kmc (2) を受けて、復号処理部 1 4 0 4 によってメモ리카ード 1 1 2 に対応する秘密復号鍵 Kmc (2) による復号処理を実行し、送信側のメモ리카ード 1 1 0 によ

って生成されたセッションキーKs 3を受理する（ステップS 3 1 4）。

メモ리카ード1 1 2のコントローラ1 4 2 0は、セッションキーKs 3の受理に応じて、セッションキー発生部1 4 1 8に対して、複製セッションにおいて受信側で発生されるべきセッションキーKs 2の生成を指示する。生成されたセッションキーKs 2は、切換スイッチ1 4 4 6中の接点 Pf および切換スイッチ1 4 4 4中の接点 Pc を経由して暗号化処理部1 4 0 6に伝達される。

暗号化処理部1 4 0 6は、復号処理部1 4 0 4からステップS 3 1 6で得られたセッションキーKs 3を受けて、切換スイッチ1 4 4 4の接点 Pc と切換スイッチ1 4 4 6の接点の切換によって得られるセッションキーKs 2と公開暗号鍵 KPm (2) をセッションキーKs 1によって暗号化し、{Ks 2//KPm (2)} Ks 3をデータベース BS 3に出力する（ステップS 3 1 6）。データベース BS 3に出力された暗号化データ {Ks 2//KPm (2)} は、携帯電話機1 0 2および1 0 0を介してメモ리카ード1 1 0のデータベース BS 3に伝達される。

メモ리카ード1 1 0においては、データベース BS 3に伝達された暗号化データを復号処理部1 4 1 2によってセッションキーKs 3を用いて復号し、メモ리카ード1 1 2に関するセッションキーKs 2および公開暗号鍵 KPm (2) を受理する（ステップS 3 1 8）。

次に、図1 3を参照して、メモ리카ード1 1 0のコントローラ1 4 2 0は、セッションキーKs 2および公開暗号鍵 KPm (2) の受理に応じて、ライセンス情報保持部1 4 4 0内のアクセス制限情報 AC 1の確認を実行する。

まず、ライセンス情報保持部1 4 4 0内に格納された対応する再生回数制限情報 Sub_Playを確認し、この値が0であるときは、すでに対応するライセンスは、再生不能の状態であるので複製セッションを終了する（ステップS 3 7 0）。一方、再生回数制限情報 Sub_Play の値が0でない場合には、複製セッションの処理が進められる（ステップS 3 2 0）。

次に、コントローラ1 4 2 0は、ライセンス情報保持部1 4 4 0内に格納された対応する所有ライセンス数 Sub_Moveを確認し、この値が0もしくは FF(h)であるときは、すでにライセンスが無い状態もしくは、ライセンスが当初から複製禁止の状態であるので複製セッションを終了する（ステップS 3 7 0）。一方、

所有ライセンス数 Sub_Move の値が 0 および FF(h) 0 以外であるときには、処理を次のステップに進める（ステップ S 3 2 2）。

5 次のステップにおいては、コントローラ 1 4 2 0 は、所有ライセンス数 Sub_Move の更新を実行する。ステップ S 3 2 4 において、複製ライセンス数の入力指示が実行され、残りライセンス数の全てについて複製を指示した場合（ステップ S 3 2 6）には、コントローラ 1 4 2 0 は、ライセンス情報保持部 1 4 4 0 からアクセス制限情報 AC 1 を取得して、所有ライセンス数 Sub_Move の値を 0 に更新する（ステップ S 3 2 8）。

10 また、ステップ S 3 2 4 において指示された複製ライセンス数が残りライセンス数よりも小さい場合には（ステップ S 3 2 6）、コントローラ 1 4 2 0 は、ライセンス情報保持部 1 4 4 0 からアクセス制限情報 AC 1 を取得して、所有ライセンス数 Sub_Move の値から、入力された複製ライセンス数を減算し、ライセンス情報保持部 1 4 4 0 内のアクセス制限情報 AC 1 を更新する（ステップ S 3 3 0）。所有ライセンス数 Sub_Move = 0 となると、以降の再生および複製が禁止
15 される。

コントローラ 1 4 2 0 は、所有ライセンス数 Sub_Move を更新した後、ライセンス情報保持部 1 4 4 0 より対応するコンテンツ ID およびライセンス ID を取得する（ステップ S 3 3 2）。

さらに、コントローラ 1 4 2 0 は、複製するコンテンツデータに対応したセッションキー Kc および再生情報に関する暗号化データ { {Kc//AC 2} Kcom//ライセンス ID//コンテンツ ID//AC 1} Km (1) の出力をメモリ 1 4 1 5 に対して指示する。メモリ 1 4 1 5 から出力された暗号化データ { {Kc//AC 2} Kcom//ライセンス ID//コンテンツ ID//AC 1} Km (1) は、復号処理部 1 4 2 2 によって復号化され、{Kc//AC 2} Kcom がデータバス BS 4 上に得られる（ステップ S 3 3 4）。
20
25

ステップ S 3 3 2 でライセンス情報保持部 1 4 4 0 から取得されたライセンス ID、コンテンツ ID およびアクセス制限情報 AC 1 と、ステップ S 3 3 4 で得られた {Kc//AC 2} Kcom は、データバス BS 4 から暗号化処理部 1 4 2 4 に取込まれて暗号化される。暗号化処理部 1 4 2 4 は、ステップ S 3 2 0 において復号処理

部 1 4 1 2 で得られたメモリカード 1 1 2 固有の公開暗号鍵 $K_{Pm}(2)$ によって、これらのデータを暗号化し、 $\{ \{ Kc//AC 2 \} Kc\ om//ライセンス\ ID//コンテンツ\ ID//AC 1 \} K_m(2)$ を出力する (ステップ S 3 3 6)。

5 データバス BS 4 に出力された暗号化データ $\{ \{ Kc//AC 2 \} Kcom//ライセンス\ ID//コンテンツ\ ID//AC 1 \} K_m(2)$ は、切換スイッチ 1 4 4 4 中の接点 Pd を介して暗号化処理部 1 4 0 6 に伝達される。暗号化処理部 1 4 0 6 は、復号処理部 1 4 1 2 によって得られたメモリカード 1 1 2 の生成したセッションキー $K_s 2$ を切換スイッチ 1 4 4 2 の接点 Pb を介して受けて、接点 Pd より受けたデータをセッションキー $K_s 2$ によって暗号化する。

10 暗号化処理部 1 4 0 6 は、 $\{ \{ \{ Kc//AC 2 \} Kcom//ライセンス\ ID//コンテンツ\ ID//AC 1 \} K_m(2) \} K_s 2$ をデータバス BS 3 に出力する (ステップ S 3 3 8)。ステップ S 3 3 8 においてデータバス BS 3 に出力された暗号化データは、携帯電話機 1 0 0 および 1 0 2 を介して、複製セッションの受信側であるメモリカード 1 1 2 に伝達される。

15 次に、図 1 4 を参照して、メモリカード 1 1 2 においては、復号処理部 1 4 1 2 においてセッションキー発生部 1 4 1 8 によって生成されたセッションキー $K_s 2$ による復号が実行され、 $\{ \{ \{ Kc//AC 2 \} Kcom//ライセンス\ ID//コンテンツ\ ID//AC 1 \} K_m(2) \}$ が受理される (ステップ S 3 4 0)。

20 公開暗号鍵 $K_{Pm}(2)$ で暗号化された $\{ \{ Kc//AC 2 \} Kcom//ライセンス\ ID//コンテンツ\ ID//AC 1 \} K_m(2)$ は、メモリ 1 4 1 5 に記録される (ステップ S 3 4 2)。さらに、復号処理部 1 4 2 2 において、メモリカード 1 1 2 に固有の秘密復号鍵 $K_m(2)$ による復号処理を実行することにより、ライセンス ID、コンテンツ ID およびアクセス制限情報 AC 1 が受理される (ステップ S 3 4 4)。

25 復号処理部 1 4 2 2 によって得られたライセンス ID、およびコンテンツ ID およびアクセス制限情報 AC 1 は、データバス BS 4 を介してライセンス情報保持部 1 4 4 0 に記録される (ステップ S 3 4 6)。

このようにして、ステップ S 3 3 8 までの処理が正常に終了することによって、再生情報が複製されたことに応答して、携帯電話機 1 0 2 を介してコンテンツデータの複製要求がさらに行なわれる (ステップ S 3 4 8)。

コンテンツデータの複製要求は携帯電話機 100 を経由してメモ리카ード 110 に伝達され、これに応答して、メモ리카ード 110 中のメモリ 1415 より対応する暗号化コンテンツデータの {Data} Kc と付加情報 Data-inf とがデータベース BS3 に出力される (ステップ S350)。

- 5 データバス BS3 に出力されたこれらのデータは、携帯電話機 100 および携帯電話機 102 を介してメモ리카ード 112 に入力され、メモ리카ード 112 中のメモリ 1415 に記録される (ステップ S352)。

暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf の記録が終了すると、携帯電話機 102 を介して複製受理が送信される (ステップ S354)。

- 10 これにより、メモ리카ード 112 および対応する携帯電話機 102 において正常に再生セッションが実行されれば、携帯電話機 102 によって、メモ리카ード 112 に記録された暗号化コンテンツデータを再生して音楽を聴取することが可能となる。

- 15 送信側の携帯電話機 100 においては、携帯電話機 102 から送信された複製受理を受信して (ステップ S356) する。

- 複製受理を受信すると、メモ리카ード 110 においては、ライセンス情報保持部 1440 内の所有ライセンス数 Sub_Move を確認し (ステップ S358)、この値が 0 である場合、すなわちライセンスが無くなった場合においては、暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf の消去もしくは保持のいずれかをタッチキー部 1108 から入力することを要求する (ステップ S360)。
- 20

- したがって、ライセンスの無くなったコンテンツデータを消去したい場合には、タッチキー部 1108 より消去を指示することにより (ステップ S362)、メモ리카ード 110 内のメモリ 1415 において、対応する暗号化コンテンツデータ {Data} Kc、付加情報 Data-inf を消去することができる (ステップ S364)。
- 25
- なお、ライセンス情報保持部 1440 内に記録された対応するコンテンツ ID 等の再生情報は、ステップ S328 にてアクセス制限情報 AC1 内の Sub_Move が更新され、Sub_Move=0 となっているため、以降の再生セッションおよび複製セッションは禁止されている。

一方、コンテンツデータ等の保持が指示された場合および、ライセンス情報保持部中の所有ライセンス数 Sub_Move が 0 以外である場合（すなわち、ライセンスが残っている場合）においては、ステップ S 3 6 4 はスキップされ、複製処理はこの段階で終了する（ステップ S 3 6 6）。

- 5 正常に複製セッションが行なわれた場合の複製処理終了ステップ S 3 6 6、もしくは認証チェック等によって複製セッションが中止された場合にはステップ S 3 0 8、S 3 2 0 および S 3 2 2 からスキップされて複製セッション全体の処理が終了する（S 3 7 0）。

- 10 このような構成とすることにより、複製セッションにおいても、受信回路側のコンテンツ再生回路（携帯電話機）およびメモリカードの認証を事前にチェックした後に、ライセンスキーや暗号化コンテンツデータの複製を実行する構成とするので、認証されていない再生回路（携帯電話機）もしくはメモリカードに対するコンテンツデータの複製の禁止を行なうことができる。

- 15 また、複製動作におけるライセンスの変化をメモリカード内で保持されるアクセス制限情報 AC 1（Sub_Move）にメモリカードが独自に反映させる構造になっている。したがって、再生情報および暗号化コンテンツデータを無制限に複製することを防止できる。

- 20 なお、暗号化コンテンツデータ {Data} Kc をメモリ 1 4 1 5 に記録された状態から、新たに配信サーバ 3 0 をアクセスし、再生情報のみの配信のみを受けることが可能な配信サービスが考えられる。このように、再生情報のみの配信を受ければ、再び、暗号化コンテンツデータ {Data} Kc を再生して、音楽を聴取できるようになる。

- 25 再生情報のみの配信処理は、フローチャートには図示されていないが、配信セッションにおける図 9 および図 1 0 において、暗号化コンテンツデータの授受に関する、ステップ S 1 4 6、S 1 4 8、S 1 5 0 および S 1 5 2 を実行しない処理に相当するため、ここでは詳細な説明を繰り返さない。

また、ステップ S 3 2 8 において、複製を目的としてライセンス情報保持部 1 4 4 0 内の再生情報を取得すると、アクセス制限情報 AC 1 内の Sub_Move の値を 0 に更新すると説明したが、当該データをライセンス情報保持部 1 4 4 0 から消

去しても同様の効果が得られる。

- 以上説明したように、実施の形態 1 に従う情報配信システムによれば、所有ライセンス数および再生可能回数といったアクセス制限情報を、配信サーバを介さずにメモ리카ード内の TRM 領域で保持更新することができる。この結果、ファイルシステムやアプリケーションプログラム等によって上位レベルからアクセス制限情報を改ざんすることができない構成とすることができるので、コンテンツデータに対する著作権保護をより強固なものとすることができる。

(実施の形態 2)

- 実施の形態 2 のデータ配信システムにおいては、実施の形態 1 のデータ配信システムの構成と異なって、再生回路共通の秘密鍵 Kcom によって復号可能な暗号化を行なわない点を特徴とする。

- すなわち、実施の形態 2 のデータ配信システムは、実施の形態 1 のデータ配信システムが具備する配信サーバ 30 内のライセンスサーバ 10 に代えてライセンスサーバ 11 を備える点で異なる。また、実施の形態 2 のデータ配信システムにおける携帯電話機の構成は、図 5 で説明した携帯電話機 100 の構成に代えて携帯電話機 101 の構成が採用される。

- 図 15 を参照して、ライセンスサーバ 11 は、ライセンスサーバ 10 と比較して、再生回路共通の秘密鍵 Kcom 保持部 322 と、秘密鍵 Kcom による暗号化処理部 324 を具備しない点で異なる。すなわち、ライセンスサーバ 11 においては、配信制御部 315 が出力するライセンスキー Kc および再生回路制御情報 AC2 は、直接暗号化処理部 326 に伝達される。その他の回路構成および動作については図 4 に示すライセンスサーバ 10 と同様であるので説明は繰返さない。

以降、ライセンスサーバ 11、認証サーバ 12 および配信キャリア 20 を合わせて配信サーバ 31 と総称することとする。

- 図 16 を参照して、実施の形態 2 に従うデータ配信システムにおいて使用される携帯電話機 101 は、実施の形態 1 で説明した携帯電話機 100 の構成と比較して、再生回路共通の秘密鍵 Kcom を保持する Kcom 保持部 1512 と秘密鍵 Kcom による復号処理部 1514 を具備しない点で異なる。

すなわち、携帯電話機 101 においては、配信サーバ 31 において秘密鍵

Kcom による暗号化処理が施されていないことに対応して、セッションキーKs 4
による復号処理を実行する復号処理部 1 5 1 0 によって直接ライセンスキーKc
が得られるため、これを復号処理部 1 5 1 0 に直接与える構成となる。その他の
回路構成および動作については携帯電話機 1 0 0 の場合と同様であるので説明は
5 繰返さない。

また、実施の形態 2 に従うデータ配信システムにおいて使用されるメモリカード
については、図 6 に示すメモリカード 1 1 0 と同一の構成であるので説明は繰
返さない。

次に、再生回路共通の秘密鍵 Kcom による暗号化を省略することによる、配信、
10 再生および複製の各セッションにおける動作の差異についてフローチャートで説
明する。

次に、図 1 7 のフローチャートを用いて、実施の形態 2 に従うデータ配信シス
テムにおける配信動作を説明する。図 1 7 においては、図 9 および図 1 0 で示し
た実施の形態 1 に従うデータ配信システムにおける配信動作のフローチャートと
15 異なる点について説明する。

図 1 7 においては、携帯電話ユーザが、メモリカード 1 1 0 を用いることで、
実施の形態 2 に従う配信サーバ 3 1 から、携帯電話機 1 0 1 を介して音楽データ
であるコンテンツデータの配信を受ける場合の動作が説明される。

図 1 7 を参照して、実施の形態 2 に従う配信動作においても、ステップ S 1 0
20 0 から S 1 2 8 までの処理は、図 1 0 で説明したフローチャートと同様であるの
で、図示および詳細な説明は繰返さない。

図 1 5 で説明したように、ステップ S 1 2 8 で得られるライセンスキーKc お
よび再生回路制御情報 AC 2 は、秘密鍵 Kcom による暗号化を施されることなくメ
モリカード 1 1 0 固有の公開暗号鍵 KPm (1) によって暗号化されるので、ステ
ップ S 1 3 0 は省略される。
25

以下、ステップ S 1 2 8 に続いて、ステップ S 1 3 2 ~ S 1 4 2 に代えて、ス
テップ S 1 3 2 a ~ S 1 4 2 a が実行される。ステップ S 1 3 2 a ~ S 1 4 2 a
のそれぞれにおいては、ステップ S 1 3 2 ~ S 1 4 2 において取り扱われるライ
センスキーKc および再生回路制御情報 AC 2 が、暗号化された形 {Kc//AC 2 }

Kcom から、そのままの形である Kc および AC 2 に代えられて取扱われる点異なる。その他の暗号化および復号処理については既に図 10 で説明したのと同様であるので説明は繰返さない。

5 図 18 には、実施の形態 2 に従うデータ配信システムにおける再生動作のフローが示される。

図 18 を参照して、実施の形態 2 に従うデータ配信システムにおいて使用される携帯電話機 101 による再生動作においては、図 11 に示した実施の形態 1 に従う再生動作と比較して、ステップ S 222 ~ S 226 に代えて、ステップ S 222a ~ S 226a が実行される点で異なる。

10 ステップ S 222a ~ S 226a のそれぞれにおいては、ステップ S 222 ~ S 226 において取り扱われるライセンスキー Kc および再生回路制御情報 AC 2 が、暗号化した形 {Kc//AC 2} Kcom から、そのままの形である Kc//AC 2 に代えられて取扱われる点異なる。その他の暗号化および復号処理については既に図 11 で説明したのと同様であるので説明は繰返さない。また、その他のステップ
15 については図 11 と同様であるので説明は繰返さない。

図 19 および図 20 には、実施の形態 2 に従うデータ配信システムにおける複製動作のフローが示される。

図 19 および図 20 においては、2つのメモ리카ード 110 および 112 の間で、実施の形態 2 に従う携帯電話機 101 および 103 を介してコンテンツデータおよびキーデータ等の複製を行なう処理を説明する。
20

携帯電話機 101 およびメモ리카ード 110 についての種類を識別するための自然数を $m=1$ および $n=1$ とし、携帯電話機 103 およびメモ리카ード 112 についての種類を識別するため自然数を $m=2$ および $n=2$ とする。また、メモ리카ード 110 および 112 を識別するための自然数 i は、実施の形態 1 と同様
25 に、それぞれ $i=1$ および $i=2$ であるものとする。

図 19 および 20 においては、図 12 から図 14 に示した実施の形態 1 に従う複製動作のフローチャートと異なる点について説明する。

図 12 で説明したステップ S 300 から S 338 までの処理は、実施の形態 2 に従う複製動作においても同様に実行されるので、図示および詳細な説明は繰り

返さない。

図 1 9 および図 2 0 を参照して、実施の形態 2 に従うデータ配信システムにおける複製セッションにおいては、図 1 3 および図 1 4 に示すステップ S 3 3 4 ~ S 3 4 4 に代えて、ステップ S 3 3 4 a ~ S 3 4 4 a が実行される点、およびステップ S 2 2 8 が省略される点で異なる。

ステップ S 3 3 4 a ~ S 3 4 4 a のそれぞれにおいては、ステップ S 3 3 4 ~ S 3 4 4 において取り扱われるライセンスキー Kc および再生回路制御情報 AC 2 が、暗号化された形 {Kc//AC 2} Kcom から、そのままの形である Kc および AC 2 に代えられて取扱われる点が異なる。また、秘密鍵 Kcom によって暗号化されることなく、ライセンスキー Kc および再生制限情報 AC2 が与えられるので、ステップ S 2 2 8 は省略される。

その他の暗号化および復号処理については既に図 1 3 および図 1 4 で説明したのと同様であるので説明は繰返さない。

その他のステップについては図 1 3 および図 1 4 と同様であるので説明は繰返さない。

このような構成とすることによって、再生回路に共通な秘密鍵 Kcom を用いない構成としても、実施の形態 1 に従うデータ配信システムと同様の効果を楽しむデータ配信システムを構築することが可能である。

[実施の形態 3]

実施の形態 3 に従うデータ配信システムにおいては、実施の形態 2 のデータ配信システムの構成とは異なって、ライセンスキー Kc および再生回路制御情報 AC2 がメモ리카ードにおいて、暗号化されることなく平文にて記録される点を特徴とする。

すなわち、実施の形態 3 に従う配信システムは、実施の形態 2 のメモ리카ード 1 1 0 に代えて、メモ리카ード 2 1 0 を備える点で異なる。配信サーバ 3 1 および携帯電話機 1 0 1 の構成は同一であるため説明は繰返さない。

図 2 1 を参照して、メモ리카ード 2 1 0 は、メモ리카ード 1 1 0 と比較して、データバス BS4 を介してメモリ 1 4 1 5 とデータの授受が行なわれない点、および、ライセンスキー Kc と再生回路制御情報 AC2 を格納する再生情報制御部 1 4

30を備える点で異なる。再生情報保持部1430は、必ずTRM領域内に設けられ、データベースBS4との間でデータの授受が可能である。

実施の形態2の場合とは異なり、公開暗号鍵 $K_{Pm}(1)$ にて暗号化された状態でメモ리카ードに伝達される、ライセンスキー K_c および再生回路制御情報AC2は、
5 メモリ1415に直接格納されない。すなわち、ライセンスキー K_c および再生回路制御情報AC2は、復号処理部1422によって復号された後、データベースBS4を介して、平文にて再生情報保持部1430に保持される。

図22を参照して、再生情報保持部1430は、ライセンス情報保持部1440と対応したN個のバンクを有し、各ライセンスに対応するライセンスキー K_c
10 および再生回路制御情報AC2をバンクごとに保持する。このとき、ライセンス情報保持部1440に保持された、同一のライセンスに対するライセンスID、コンテンツIDおよびアクセス制限情報AC1を保持したバンクと対応したバンクを用いる。

その他の部分の構成については、メモ리카ード110と同様であるため詳細な説明は省略する。なお、メモ리카ードに対応して定められる自然数 i 、および m
15 は、本来、メモ리카ード110と同一の値になり得ないが、説明を簡略化するために、以下においては、これらの自然数 i および m は、実施の形態1および2におけるメモ리카ード110と同様に、 $i=1$ および $m=1$ であるものとして説明する。

20 実施の形態3に従う配信動作については、フローチャートは図示されていないが、実施の形態2における図17の配信動作時のフローチャートにおいて、ライセンスの記録を行なうステップS140aおよびS142aにおける処理を変更すればよい。

ステップS140aに相当するステップにおいては、暗号化データ
25 $\{K_c//AC1//ライセンスID//コンテンツID//AC2\} K_{m(1)}$ を復号処理部1422において秘密復号鍵 $K_{m(1)}$ を用いて復号し、得られたライセンスキー K_c および再生回路制御情報AC2を再生情報保持部1430に記録する。さらに、ステップS142aに相当するステップにおいては、ステップS140aに相当するステップにおける復号処理で得られたライセンスID、コンテンツIDおよびアクセス制限

情報 AC1 を、ライセンス保持部情報保持部 1 4 4 0 中の再生情報保持部 1 4 3 0 と対応するバンクに記録する。再生動作の他のステップにおける処理は、実施の形態 2 の場合と同様であるため説明は繰り返さない。

5 同様に、実施の形態 3 に従う再生動作については、フローチャートは図示されていないが、実施の形態 2 における図 1 8 の再生動作時のフローチャートにおいて、メモリ 1 4 1 5 からライセンスキー Kc、再生回路制御情報 AC2 を取得するステップ S 2 2 2 a における処理内容が変更される。すなわち、ステップ S 2 2 2 a に相当するステップにおいて、再生情報保持部 1 4 3 0 からライセンスキー Kc、再生回路制御情報 AC2 を取得する。再生動作の他のステップにおける処理は、実施の形態 2 の場合と同様であるため説明は繰り返さない。

このように、実施の形態 3 に従う配信システムは、実施の形態 2 に従う配信システムに対してメモ리카ード 2 1 0 の内部処理が異なるのみであり、実施の形態 2 と互換性があり、相互に運用することができる。

同様に、実施の形態 3 に従う複製動作については、フローチャートが図示されていないが、配信動作および再生動作と同様に、実施の形態 2 における図 1 9 および図 2 0 の複製動作時のフローチャートにおいて、メモリ 1 4 1 5 からライセンスキー Kc、再生回路制御情報 AC2 を取得するステップ S 3 3 4 a、ライセンスの記録を行なうステップ S 3 4 2 a および S 3 4 4 a における処理を変更すればよい。すなわち、ステップ S 3 4 2 a に相当するステップにおいては、暗号化データ {Kc//AC2//ライセンス ID//コンテンツ ID//AC1} Km(2) を復号処理部 1 4 2 2 において秘密復号鍵 Km(2) を用いて復号し、得られたライセンスキー Kc および再生回路制御情報 AC2 を再生情報保持部 1 4 3 0 に記録する。さらに、ステップ S 3 4 4 a に相当するステップにおいては、ステップ S 3 4 2 a に相当するステップにおける復号処理で得られたライセンス ID、コンテンツ ID およびアクセス制限情報 AC1 を、ライセンス保持部情報保持部 1 4 4 0 中の再生情報保持部 1 4 3 0 と対応するバンクに記録する。

25 なお、実施の形態 2 における配信システムにおいては、メモ리카ード内の動作が異なるのみであるため、実施の形態 2 のメモ리카ード 1 1 0 と実施の形態 3 のメモ리카ード 2 1 0 とは相互互換のあるメモ리카ードであり、その意味において

実施の形態 2 と実施の形態 3 との配信システムは同一の配信システムで運用することができる。

また、このような実施の形態 3 に従うメモリカード 2 1 0 の適用は、実施の形態 1 に従う配信システムとの組合せにおいても実行することができる。すなわち、
5 ライセンスキー Kc および再生回路制御情報 AC2 を鍵 Kcom によって暗号化された {Kc//AC 2} Kcom の状態で、再生情報保持部 1 4 3 0 に記録することも可能である。

以下に、このような場合における実施の形態 1 に従う配信システムにおける処理動作からの変更点を説明する。

10 実施の形態 3 を実施の形態 1 と組合せた場合の配信動作については、実施の形態 1 における図 1 0 フローチャートにおいて、ライセンスの記録を行なうステップ S 1 4 0 および S 1 4 2 における処理を変更すればよい。

ステップ S 1 4 0 に相当するステップにおいては、暗号化データ { {Kc//AC 2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km(1) を復号処理部 1 4 2 2 に
15 おいて秘密復号鍵 Km(1) を用いて復号し、得られたライセンスキー Kc および再生回路制御情報 AC2 を再生情報保持部 1 4 3 0 に記録する。さらに、ステップ S 1 4 2 に相当するステップにおいては、ステップ S 1 4 0 に相当するステップにおける復号処理で得られたライセンス ID、コンテンツ ID およびアクセス制限情報 AC1 を、ライセンス保持部情報保持部 1 4 4 0 中の再生情報保持部 1 4 3 0 と対
20 応するバンクに記録する。再生動作の他のステップにおける処理は、実施の形態 1 の場合と同様であるため説明は繰り返さない。

同様に、実施の形態 3 を実施の形態 1 と組合せた場合の再生動作については、実施の形態 1 における図 1 1 の再生動作時のフローチャートにおいて、メモリ 1 4 1 5 からライセンスキー Kc、再生回路制御情報 AC2 を取得するステップ S 2 2 2 における処理内容が変更される。すなわち、ステップ S 2 2 2 に相当するステップにおいて、ライセンスキー Kc、再生回路制御情報 AC2 を {Kc//AC 2} Kcom の形で再生情報保持部 1 4 3 0 から取得する。再生動作の他のステップにおける
25 処理は、実施の形態 1 の場合と同様であるため説明は繰り返さない。

同様に、実施の形態 3 を実施の形態 1 と組合せた場合の複製動作については、

配信動作および再生動作と同様に、実施の形態 1 における図 1 3 および図 1 4 の複製動作時のフローチャートにおいて、メモリ 1 4 1 5 からライセンスキー Kc および再生回路制御情報 AC2 を {Kc//AC 2} Kcom の形で取得するステップ S 3 3 4、ライセンスの記録を行なうステップ S 3 4 2 および S 3 4 4 における処理
5 を変更すればよい。すなわち、ステップ S 3 4 2 に相当するステップにおいては、暗号化データ { {Kc//AC 2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km(2) を復号処理部 1 4 2 2 において秘密復号鍵 Km(2) を用いて復号し、得られた {Kc//AC 2} Kcom を再生情報保持部 1 4 3 0 に記録する。さらに、ステップ S 3 4 4 に相当するステップにおいては、ステップ S 3 4 2 に相当するステップに
10 における復号処理で得られたライセンス ID、コンテンツ ID およびアクセス制限情報 AC1 を、ライセンス保持部情報保持部 1 4 4 0 中の再生情報保持部 1 4 3 0 と対応するバンクに記録する。

このように、実施の形態 3 に従う配信システムは、実施の形態 1 に従う配信システムに対してメモ리카ード 2 1 0 の内部処理が異なるのみであり、実施の形態
15 1 と互換性があり、相互に運用することができる。

なお、実施の形態 1 における配信システムにおいては、メモ리카ード内の動作が異なるのみであるため、実施の形態 1 のメモ리카ード 1 1 0 と実施の形態 3 のメモ리카ード 2 1 0 とは相互互換のあるメモ리카ードであり、その意味において
20 実施の形態 1 と実施の形態 3 とを組合せて同一の配信システムで運用することができる。

なお、図 2 1 においては、TRM 領域に配置される再生情報保持部 1 4 3 0 およびライセンス保持部情報保持部 1 4 4 0 を独立した機能を有するブロックとして示したが、両者を共通のメモリとして配置することも可能である。また、実施の
形態 1 で述べたように、メモリ 1 4 1 5 を TRM 領域に配置することも可能である
25 が、この場合において、メモリ 1 4 1 5、再生情報保持部 1 4 3 0 およびライセンス保持部情報保持部 1 4 4 0 を共通の同一メモリ上に設けることも可能である。

なお、以上で説明したすべての実施の形態においては、複製動作時において、一度に複数のライセンスが複製できる構成について説明したが、一度の複製動作では、1 つのライセンスが複製可能なように構成することも可能である。この場

合においては、実施の形態 1 における図 1 3 ならびに、実施の形態 2 および 3 における図 2 0 に示したフローチャートからステップ S 3 2 4 を省略して、ステップ S 3 2 6 において、複製ライセンス数が “1” であるとして判断する処理とすればよい。

- 5 また、ライセンスの複製は、アクセス制限情報 AC1 の所有ライセンス数 Sub__move の制約上必ず制限を受けるように説明したが、コンテンツデータの著作権を所有する著作権者が自由に複製することを許可した場合には、自由な複製が可能となる。この場合には、たとえば所有ライセンス数 Sub__move に新たな値、たとえば FE(h) を追加して、Sub__move=FE(h) であれば複製自由とし、図 1 3 に示したフローチャート中のステップ S 3 2 2 の判断処理において、Sub__move=FE(h) の場合に新しい分岐を設けて、ライセンス処理部から AC1 を取得する処理を得た後、Sub__move=FE(h) であればステップ S 3 3 2 に移行する処理を行なうことで実現することができる。
- 10

- 15 また、以上で説明したすべての実施の形態においては、配信動作において、携帯電話機 1 0 0 から 2 つの認証データ {KPmc(1)//Cmc(1)} KPma および {KPp(1)//Cp(1)} KPma を送信して配信サーバ 1 0 において 2 つの認証データに対して認証処理をする構成について説明した。

- 20 しかし、メモリカード 1 1 0 は着脱可能であることから、音楽を再生する場合にコンテンツ再生回路が必ずしも配信を受けた携帯電話機 1 0 0 である必然性がない。さらに、メモリカード 1 0 0 が再生動作において再生するコンテンツ再生回路の認証データ {KPp(1)//Cp(1)} KPma によって認証処理を行なっているので、配信サーバ 1 0 においてコンテンツ再生回路の認証データ {KPp(1)//Cp(1)} KPma によってコンテンツ再生回路（携帯電話機 1 0 0）の認証処理を行なわなくてもセキュリティの低下にはつながらない。

- 25 したがって、配信サーバ 1 0 に対して、メモリカード 1 0 0 の認証データ {KPmc(1)//Cmc(1)} KPma のみを送信し、配信サーバ 1 0 においては、配信先のメモリカード 1 1 0 の認証データ {KPmc(1)//Cmc(1)} KPma のみを中心にして復号し認証処理を行なう構成としても同様の効果を得ることができる。

この場合には、すべての実施の形態が参照する図 9 に示されたフローチャート

において、ステップ S 1 0 4、S 1 0 6、S 1 0 8、S 1 1 0 の各処理において、携帯電話機（コンテンツ再生回路）1 0 0 の認証データ {K_{Pp}(1)//C_p(1)} K_{Pma}、公開暗号鍵 K_{Pp}(1) およびクラス証明書 C_p(1) に対する処理を省略することによって、コンテンツ再生回路に対する認証を省略した認証処理を行なうことができる。

- 5 今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

10 産業上の利用可能性

この発明によるデータ配信システムおよび記録装置は、携帯電話機のような移動通信端末を利用したデータ配信に用いることができる。

請求の範囲

1. データ配信システムであって、
暗号化コンテンツデータ（{Data} Kc）と、前記暗号化コンテンツデータを復
号して平文のコンテンツデータ（Data）を得るための復号鍵であるライセンスキ
5 ー（Kc）を配信するためのコンテンツ供給装置（10, 11）と、
前記コンテンツ供給装置からの前記配信を受ける複数の端末（100, 10
1）とを備え、
前記コンテンツ供給装置は、
外部との間でデータを授受するための第1のインタフェース部（350）と、
10 前記配信が要求された場合において、アクセス制限情報（AC1）を生成して、
少なくとも前記ライセンスキーを含む再生情報（Kc//AC2, {Kc//AC2} Kcom）と前
記アクセス制限情報とを前記第1のインタフェース部を介して出力するための配
信制御部（315）とを含み、
各前記端末は、
15 外部との間でデータを授受するための第2のインタフェース部（1102）と、
前記第2のインタフェース部を介して、前記暗号化コンテンツデータと前記再
生情報と前記アクセス制限情報とを受けて記録する配信データ解読部（110,
210）とを含み、
前記配信データ解読部は、
20 前記暗号化コンテンツデータ、前記再生情報および前記アクセス制限情報を記
録するための記憶部（1415, 1430, 1440）と、
外部から前記再生情報の出力が指示された場合に、前記記憶部に記録された前
記アクセス制限情報に基づいて前記出力の可否を判断する制御部（1420）と
を有する、データ配信システム。
- 25 2. 各前記端末（100, 101）は、コンテンツ再生部をさらに含み、
前記コンテンツ再生部は、
外部からコンテンツデータの再生動作が指示された場合において、前記配信デ
ータ解読部（110, 210）から前記再生情報（Kc//AC2, {Kc//AC2} Kcom）お
よび前記暗号化コンテンツデータ（{Data} Kc）を受けて、前記ライセンスキー

(Kc) によって前記暗号化コンテンツデータを復号して再生するコンテンツデータ再生部 (1516, 1518) を有し、

前記アクセス制限情報 (AC1) は、前記配信データ解読部から前記コンテンツ再生部への、前記再生情報の出力回数を制限する再生制御情報 (Sub_Play) を含み、

前記制御部 (1420) は、前記再生動作が指示された場合において、前記記憶部に記録された前記再生制御情報に基づいて、前記再生情報の出力の可否を判断するとともに、前記再生情報の出力後、必要に応じて前記再生制御情報を更新できる、請求の範囲第1項に記載のデータ配信システム。

3. 前記アクセス制限情報 (AC1) は、前記配信データ解読部 (110, 210) から他の配信データ解読部 (112) に対しての、前記再生情報 (Kc//AC2, {Kc//AC2} Kcom) の複製可能回数を制限する複製制限情報 (Sub_Move) を含み、

前記制御部 (1420) は、他の配信データ解読部に対して前記再生情報を複製する複製動作が外部から指示された場合において、前記記憶部に記録された前記複製制限情報に基づいて前記再生情報の出力の可否を判断するとともに、前記再生情報の出力後、必要に応じて前記複製制限情報を更新できる、請求の範囲第1項に記載のデータ配信システム。

4. 前記コンテンツ供給装置 (10, 11) は、

認証鍵 (KPma) によって復号可能な状態に暗号化された、前記配信データ解読部 (110, 210) に対応して予め定められる第1の公開暗号鍵 (KPmc(m)) を、前記第1のインタフェース部 (350) を介して受けて復号処理するための第1の復号処理部 (312) と、

前記暗号化コンテンツデータおよび前記ライセンスキーの少なくとも一方の通信ごとに更新される第1の共通鍵 (Ks1) を生成する第1のセッションキー生成部 (316) と、

前記第1の共通鍵によって暗号化されて、前記第1のインタフェース部を介して返信される第2の公開暗号鍵 (KPm(i)) および第2の共通鍵 (Ks2) を復号抽出するためのセッションキー復号部 (320) と、

前記再生情報 (Kc//AC2, {Kc//AC2} Kcom) および前記アクセス制限情報 (AC1) を、

前記セッションキー復号部により復号された前記第 2 の公開暗号鍵によって暗号化する第 1 のライセンスデータ暗号化処理部（3 2 6）と、

前記第 1 のライセンスデータ暗号化処理部の出力を、前記セッションキー復号部により復号された前記第 2 の共通鍵によってさらに暗号化して前記第 1 のインタフェース部に与え配信するための第 2 のライセンスデータ暗号化処理部（3 2 8）とをさらに含み、

前記配信データ解読部（1 1 0, 2 1 0）は、

前記認証鍵によって復号可能な状態に暗号化された、前記配信データ解読部に対応して定められる前記第 1 の公開暗号鍵を保持し、少なくとも前記ライセンスキーを受信する場合に出力する第 1 の認証データ保持部（1 4 0 0）と、

前記第 1 の公開暗号鍵によって暗号化されたデータを復号するための第 1 の秘密復号鍵（ $K_{mc}(m)$ ）を保持する第 1 の鍵保持部（1 4 0 2）と、

前記第 1 の公開暗号鍵によって暗号化された前記第 1 の共通鍵を受けて、前記第 1 の秘密復号鍵によって復号処理するための第 1 の復号処理部（1 4 0 4）と、
前記第 2 の公開暗号鍵を保持する第 2 の鍵保持部（1 4 1 6）と、

前記暗号化コンテンツデータおよび前記ライセンスキーの少なくとも一方の通信ごとに更新される前記第 2 の共通鍵（ K_{s2} ）を生成する第 2 のセッションキー発生部（1 4 1 8）と、

前記第 2 の共通鍵および前記第 2 の公開暗号鍵を前記第 1 の共通鍵によって暗号化し、前記第 2 のインタフェース部（1 2 0 2）に出力するための第 1 の暗号化処理部（1 4 0 6）と、

前記コンテンツ供給装置から配信される、前記第 2 の共通鍵および前記第 2 の公開暗号鍵によって暗号化された、前記再生情報および前記アクセス制限情報を受けて、前記第 2 の共通鍵によって復号するための第 2 の復号処理部（1 4 1 2）と、

前記第 2 の公開暗号鍵によって暗号化されたデータを復号するための第 2 の秘密復号鍵（ $K_{m(i)}$ ）を保持する第 3 の鍵保持部（1 4 2 1）と、

暗号化された、前記再生情報および前記アクセス制限情報を、第 2 の秘密復号鍵によって復号するための第 3 の復号処理部（1 4 2 2）とをさらに有し、

前記記憶部（１４１５，１４３０，１４４０）は、前記再生情報を、前記第２の公開暗号鍵によって暗号化された状態および前記第３の復号処理部によって復号された状態のいずれか一方の状態で記録するための第１の記憶ブロック（１４１５，１４３０）と、

- ５ 前記アクセス制限情報を記録するための第２の記憶ブロック（１４４０）とを有する、請求の範囲第１項に記載のデータ配信システム。

５． 前記第２のセッションキー発生部（１４１８）は、外部から指示されるコンテンツデータの再生動作に応じて、第３の共通鍵（Ks3）を生成し、

- １０ 前記記憶部（１４１５，１４３０，１４４０）は、前記制御部（１４２０）に制御されて、前記再生動作が指示されるのに応じて、前記暗号化コンテンツデータ（{Data} Kc）および前記再生情報を出力し、

前記第３の復号処理部（１４２２）は、前記再生動作において、前記第１の記憶ブロックから出力された前記再生情報が暗号化されている場合に、復号を行なって前記再生情報（Kc//AC2，{Kc//AC2} Kcom）を抽出し、

- １５ 前記第２の復号処理部（１４１２）は、前記再生動作において、前記第３の共通鍵によって暗号化されて前記端末から返信されるデータを復号して、前記再生動作を行なう前記端末において前記再生情報の通信ごとに更新される第４の共通鍵（Ks4）を抽出し、

- ２０ 前記第１の暗号化処理部（１４０６）は、前記再生動作において、前記第３の復号処理部および前記第１の記憶ブロックのいずれか一方から前記再生情報を受けて、前記第２の復号処理部（１４１２）で抽出された前記第４の共通鍵によって暗号化し、

各前記端末（１００，１０１）は、コンテンツ再生部をさらに備え、

前記コンテンツ再生部は、

- ２５ 前記認証鍵によって復号可能な状態に暗号化された、前記コンテンツ再生部に対応して予め定められる、第３の公開暗号鍵（Kp(i)）を保持し、前記再生動作に応じて前記配信データ解読部に対して出力する第２の認証データ保持部（１５００）と、

前記第４の共通鍵を生成する第３のセッションキー発生部（１５０８）と、

前記配信データ解読部から送信される、前記第4の共通鍵によって暗号化された前記再生情報から前記再生情報を復号抽出するための第4の復号処理部（1510）と、

5 前記再生動作が指示された場合において、前記配信データ解読部（110, 210）からの前記暗号化コンテンツデータを受けて、前記再生情報に含まれる前記ライセンスキー（Kc）により前記暗号化コンテンツデータを復号して再生するためのコンテンツデータ再生部（1516, 1518）と、

前記第3の公開暗号鍵によって暗号化されたデータを復号化するための第3の秘密復号鍵（Kp(i)）を保持する第4の鍵保持部（1502）と、

10 前記第3の公開暗号鍵によって暗号化されて前記配信データ解読部から返信されるデータを復号して前記第3の共通鍵を得るための第5の復号処理部（1504）と、

前記第5の復号処理部から受ける前記第3の共通鍵によって、前記第4の共通鍵を暗号化して前記配信データ解読部に対して出力する第2の暗号化処理部（1506）とを有し、

前記配信データ解読部は、

暗号化された前記第3の公開暗号鍵を前記コンテンツ再生部から受けて、前記認証鍵によって復号処理するための認証処理部（1408）と、

20 前記制御部に制御されて、前記認証処理部から受ける前記第3の公開暗号鍵によって前記第3の共通鍵を暗号化して、対応する前記コンテンツ再生部に対して出力する第3の暗号化処理部（1410）とをさらに有し、

前記アクセス制限情報（ACI）は、前記配信データ解読部から前記コンテンツデータ再生部への、前記再生情報の出力回数を制限する再生制御情報（Sub_Move）を含み、

25 前記制御部（1420）は、前記再生動作が指示された場合において前記配信データ解読部の各部の動作を制御し、前記第2の記憶ブロックに記録された前記再生制御情報に基づいて前記再生情報の出力の可否を判断するとともに、前記再生情報の出力後、必要に応じて前記再生制御情報を更新可能である、請求の範囲第4項に記載のデータ配信システム。

6. 前記認証処理部（1408）は、他の配信データ解読部（102）に対して前記再生情報を複製する複製動作が外部から指示された場合において、前記他の配信データ解読部に対応する前記第1の公開暗号鍵（ $K_{Pm(m)}$ ）を復号処理によって取得し、
- 5 前記配信データ解読部および前記他の配信データ解読部にそれぞれ対応する複数の前記第2のセッションキー発生部は、外部から指示される前記複製動作に応じて、前記第3および第2の共通鍵（ K_{s3} , K_{s2} ）をそれぞれ生成し、
- 前記第3の暗号化処理部（1410）は、前記複製動作において、前記他の配信データ解読部に対応する前記第1の公開暗号鍵によって、前記配信データ解読部に対応する前記第3の共通鍵を暗号化して前記他の配信データ解読部に対して出力し、
- 10 前記第2の復号処理部（1412）は、前記複製動作において、前記配信データ解読部に対応する前記第3の共通鍵で暗号化されて前記他の配信データ解読部から返信されるデータを復号して、前記他の配信データ解読部で生成された前記第2の共通鍵および前記他の配信データ解読部に対応する前記第2の公開暗号鍵（ $K_{Pm(i)}$ ）を取得し、
- 15 前記第1の記憶ブロック（1415, 1430）は、前記制御部（1420）に制御されて、前記複製動作が指示されるのに応じて、前記再生情報を出力し、
- 前記第3の復号処理部（1422）は、前記複製動作において、前記第1の記憶ブロックから出力された前記再生情報が暗号化されている場合に、復号を行なって前記再生情報（ $K_c//AC2$, $\{K_c//AC2\} K_{com}$ ）を抽出し、
- 20 前記配信データ解読部（110, 210）は、
- 前記複製動作が外部から指示された場合において、前記第3の復号処理部および前記第1の記憶ブロックのいずれか一方から受けた前記再生情報を、前記他の配信データ解読部に対応する前記第2の公開暗号鍵によって暗号化するための第4の暗号化処理部（1424）をさらに有し、
- 25 前記第1の暗号化処理部（1406）は、前記複製動作において、前記第2の復号処理部（1412）によって取得された前記第2の共通鍵と、前記第4の暗号化処理部の出力とを受けて、前記第4の暗号化処理部の出力を前記第2の共通

鍵によってさらに暗号化して前記他の配信データ解読部に出力し、

前記アクセス制限情報 (AC1) は、前記配信データ解読部から他の配信データ解読部に対しての、前記再生情報の複製可能回数を制限する複製制限情報 (Sub_move) を含み、

- 5 前記制御部 (1420) は、前記複製動作時において前記配信データ解読部の各部の動作を制御し、前記第2の記憶ブロックに記録された前記複製制限情報に基づいて前記再生情報の出力の可否を判断するとともに、前記再生情報の出力後、必要に応じて前記複製制限情報を更新する、請求の範囲第5項に記載のデータ配信システム。

- 10 7. 前記コンテンツ供給装置 (10) は、

前記コンテンツ再生部にて再生可能な共通秘密鍵 (Kcom) を保持する第5の鍵保持部 (322) と、

- 15 前記再生情報 (Kc//AC2, {Kc//AC2} Kcom) を前記共通秘密鍵によって暗号化し、前記第1のライセンスデータ暗号化処理部 (326) に対して出力する第3のライセンスデータ暗号化部 (324) とをさらに含み、

前記コンテンツ再生部は、

前記共通秘密鍵を保持する第6の鍵保持部 (1512) と、

- 20 前記第4の復号処理部 (1510) の出力を受けて、前記第6の鍵保持部に保持された前記共通秘密鍵によって前記再生情報を復号し、前記ライセンスキー (Kc) を抽出して前記コンテンツデータ再生部 (1516, 1518) に対して出力するための第6の復号処理部 (1514) をさらに有する、請求の範囲第5項に記載のデータ配信システム。

8. 前記コンテンツ供給装置 (10) は、

- 25 前記コンテンツデータ再生部にて再生可能な第4の公開暗号鍵を保持する第5の鍵保持部と、

前記再生情報を前記第4の公開暗号鍵にて暗号化し、前記第1のライセンスデータ暗号化処理部に対して出力する第3のライセンスデータ暗号化部をさらに含み、

前記コンテンツ再生部は、

前記第４の公開暗号鍵によって暗号化された前記再生情報を復号できる第４の秘密復号鍵を保持する第６の鍵保持部と、

前記第４の復号処理部の出力を受けて、前記第６の鍵保持部に保持された前記第４の秘密復号鍵によって前記再生情報（AC//Kc2）を復号し、前記ライセンス
5 キー（Kc）を抽出して前記コンテンツデータ再生部（１５１６、１５１８）に対して出力するための第６の復号処理部をさらに含む、請求の範囲第５項に記載のデータ配信システム。

9. 前記配信データ解読部（１１０、２１０）は、前記端末（１００、１０１）に着脱可能な記録装置である、請求の範囲第１項に記載のデータ配信システム。
10

10. 前記記録装置は、メモリカードである、請求の範囲第９項に記載のデータ配信システム。

11. 前記第１のインタフェース部（３５０）と前記第２のインタフェース部（１２０２）とは、携帯電話網によって接続される、請求の範囲第１項に記載のデータ配信システム。
15

12. 前記記憶部（１４１５、１４３０、１４４０）は、外部から直接アクセス不可能なセキュリティー領域（TRM）内に配置される、請求の範囲第１項に記載のデータ配信システム。

13. 前記記憶部（１４１５、１４３０、１４４０）は、
20 前記暗号化コンテンツデータを記録するための第１の記憶ブロック（１４１５）と、

前記アクセス制限情報を記録するための第２の記憶ブロック（１４４０）とを含み、

前記第１の記憶ブロックは、前記再生情報を暗号化された状態でさらに記録し、
25 前記第２の記憶ブロックは、外部から直接アクセス不可能なセキュリティー領域（TRM）内に配置される、請求の範囲第１項に記載のデータ配信システム。

14. 前記記憶部（１４１５、１４３０、１４４０）は、
前記暗号化コンテンツデータを記録するための第１の記憶ブロック（１４１５）と、

前記アクセス制限情報および前記再生情報を記録するための第2の記憶ブロック（1430, 1440）とを含み、

前記第2の記憶ブロックは、外部から直接アクセス不可能なセキュリティー領域（TRM）内に配置される、請求の範囲第1項に記載のデータ配信システム。

5 15. 前記配信制御部（315）は、配信先の前記配信データ解読部（110, 120）を認証した後に、前記再生情報（Kc//AC2, {Kc//AC2} Kcom）と前記アクセス制限情報（AC1）とを前記第1のインタフェース部（350）を介して出力する、請求の範囲第1項に記載のデータ配信システム。

10 16. 前記配信データ解読部（110, 120）は、外部から前記再生情報（Kc//AC2, {Kc//AC2} Kcom）の出力が指示された場合に、出力先を認証した後に、前記再生情報を前記第2のインタフェース部（1102）を介して出力する、請求の範囲第1項に記載のデータ配信システム。

15 17. 前記制御部（1420）は、前記複製動作において、他の配信データ解読部（112）に対しての前記アクセス制限情報（AC1）を前記再生情報（Kc//AC2, {Kc//AC2} Kcom）とともに出力し、

前記制御部は、前記他の配信データ解読部に対する前記複製制限情報（Sub_Move）を生成するとともに、前記記憶部（1415, 1430, 1430）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更した前記アクセス制限情報を前記他の配信データ解読部に対して出力する、請求の範囲第3項に記載のデータ配信システム。

20 18. 前記制御部（1420）は、前記複製動作において、他の配信データ解読部（112）に対しての前記アクセス制限情報（AC1）を前記再生情報（Kc//AC2, {Kc//AC2} Kcom）とともに出力し、

25 前記制御部は、前記他の配信データ解読部に対する前記複製制限情報（Sub_Move）を生成するとともに、前記記憶部（1415, 1430, 1430）に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更し、

前記第4の暗号化処理部は、変更した前記アクセス制限情報を暗号化して、前記再生情報とともに前記第1の暗号化処理部へ与える、請求の範囲第6項に記載

のデータ配信システム。

19. 記録装置であって、

外部との間でデータを授受するためのインタフェース部（1202）と、

前記インタフェース部を介して入力される、格納データ（Kc//AC2, {Kc//AC2}

5 Kcom)および前記格納データの前記記録装置からの出力を制御するためのアクセス制限情報（AC1）を記録するための記憶部（1415, 1430, 1440）と、

外部から前記格納データの出力が指示された場合に、前記記憶部に記録された前記アクセス制限情報に基づいて前記出力の可否を判断する制御部（1420）

10 とを備える、記録装置。

20. 前記アクセス制限情報（AC1）は、前記記録装置から他の機器（100, 101）への前記格納データ（Kc//AC2, {Kc//AC2} Kcom)の出力回数を制限する出力回数制御情報（Sub_Play）を含み、

前記制御部（1420）は、前記他の機器に対する前記格納データの出力が指示された場合において、前記出力回数制御情報に基づいて前記出力の可否を判断するとともに、前記出力後、必要に応じて前記出力回数制御情報を更新可能である、請求の範囲第19項に記載の記録装置。

21. 前記アクセス制限情報（AC1）は、他の前記記録装置（112）に対する前記格納データ（Kc//AC2, {Kc//AC2} Kcom)の複製可能回数を制限する複製制限情報（Sub_Move）を含み、

前記制御部（1420）は、前記他の記録装置に対する前記格納データの複製指示が外部から指示された場合において、前記複製制限情報に基づいて前記格納データの出力の可否を判断するとともに、前記出力後、必要に応じて前記複製制限情報を更新可能である、請求の範囲第19項に記載の記録装置。

22. 前記記憶部は、前記アクセス制限情報（AC1）を記録するための記憶ブロック（1440）を有し、

前記記録装置は、

前記記録装置に対応して予め定められる公開暗号鍵（K_{Pm}(i)）によって暗号化されたデータを復号するための秘密復号鍵（K_m(i)）を保持する秘密鍵保持部

(1 4 2 1) と、

前記インタフェース部 (1 2 0 2) を介して入力される、前記公開暗号鍵によって暗号化された前記アクセス制限情報 (AC1) を復号して、前記記憶ブロックに与えるアクセス制限情報復号部 (1 4 2 2) とをさらに備える、請求の範囲第 1 9 項に記載の記録装置。

2 3. 前記記憶ブロック (1 4 3 0, 1 4 4 0) は、外部から直接アクセス不可能なセキュリティ領域 (TRM) 内に配置される、請求の範囲第 2 2 項に記載の記録装置。

2 4. 認証鍵 (KPma) によって復号可能な状態に暗号化された、前記記録装置に対応して定められる第 1 の公開暗号鍵 (KPmc(m)) を保持し、前記格納データ (Kc//AC2, {Kc//AC2} Kcom) および前記アクセス制限情報 (AC1) を受信する場合において前記インタフェース部 (1 2 0 2) を介して外部に出力する認証データ保持部 (1 4 0 0) と、

前記第 1 の公開暗号鍵によって暗号化されたデータを復号化するための第 1 の秘密復号鍵 (Kmc(m)) を保持する第 1 の鍵保持部 (1 4 4 2) と、

前記第 1 の公開暗号鍵によって暗号化された第 1 の共通鍵 (Ks1) を前記インタフェース部を介して外部から受けて、復号処理するための第 1 の復号処理 (1 4 0 4) と、

前記記録装置ごとに異なる第 2 の公開暗号鍵 (KPm(i)) を保持する第 2 の鍵保持部 (1 4 1 6) と、

前記格納データの通信ごとに更新される第 2 の共通鍵 (Ks2) を生成するセッションキー発生部 (1 4 1 8) と、

前記第 2 の共通鍵および前記第 2 の公開暗号鍵を前記第 1 の共通鍵によって暗号化し、前記インタフェース部を介して外部に出力するための第 1 の暗号化処理部 (1 4 0 6) と、

前記インタフェース部を介して、前記第 2 の共通鍵および前記第 2 の公開暗号鍵によって暗号化されて入力される前記格納データおよび前記アクセス制限情報を受けて、前記第 2 の共通鍵によって復号するための第 2 の復号処理部 (1 4 1 2) と、

前記第 2 の公開暗号鍵によって暗号化されたデータを復号するための第 2 の秘密復号鍵 ($K_m(i)$) を保持する第 3 の鍵保持部 (1 4 2 1) と、

暗号化された、前記格納データおよび前記アクセス制限情報を、前記第 2 の秘密復号鍵によって復号するための第 3 の復号処理部 (1 4 2 2) とをさらに備え、

5 前記記憶部 (1 4 1 5, 1 4 3 0, 1 4 4 0) は、前記格納データを、前記第 2 の公開暗号鍵によって暗号化された状態および、前記第 3 の復号処理部によって復号された状態のいずれか一方の状態記録する、請求の範囲第 1 9 項に記載の記録装置。

2 5. 前記セッションキー発生部 (1 4 1 8) は、外部から指示される、他の機器 (1 0 0, 1 0 1) への前記格納データ ($K_c//AC2$, $\{K_c//AC2\} K_{com}$) の出力指示である第 1 の出力指示に応じて、第 3 の共通鍵 (K_{s3}) を生成し、

前記記録装置は、

前記認証鍵 (K_{Pma}) によって復号可能な状態に暗号化された、前記他の機器に対応して予め定められる第 3 の公開暗号鍵 ($K_{Pp}(n)$) を前記インタフェース部 (1 2 0 2) を介して受けて、前記認証鍵によって復号処理するための認証処理部 (1 4 0 8) と、

前記第 1 の出力指示に応じて、前記認証処理部から受ける前記第 3 の公開暗号鍵によって前記第 3 の共通鍵を暗号化して、前記他の機器に対して出力する第 2 の暗号化処理部 (1 4 1 0) とをさらに備え、

20 前記インタフェース部は、前記第 1 の出力指示に応じて、前記第 3 の共通鍵によって暗号化されて返信される、前記他の機器において生成された第 4 の共通鍵 (K_{s4}) を受けて前記第 2 の復号処理部 (1 4 1 2) に伝達し、

前記第 2 の復号処理部は、前記第 1 の出力指示に応じて、前記セッションキー発生部から受けた前記第 3 の共通鍵によって、前記第 3 の共通鍵によって暗号化された前記第 4 の共通鍵を抽出し、

25 前記記憶部は、前記制御部 (1 4 2 0) に制御されて、前記第 1 の出力指示に応じて、前記格納データを出力し、

前記第 3 の復号処理部 (1 4 2 2) は、前記第 1 の出力指示に応じて、前記記憶部から出力された前記格納データが暗号化されている場合に、復号を行なって

前記格納データを抽出し、

前記第 2 の復号処理部 (1 4 1 2) は、前記第 1 の出力指示に応じて、前記第 3 の共通鍵によって暗号化されて前記端末から返信されるデータを復号して、前記再生動作を行なう前記端末において前記格納データの通信ごとに更新される第 4 の共通鍵 (Ks4) を抽出し、

前記第 1 の暗号化処理部 (1 4 0 6) は、前記第 1 の出力指示に応じて、前記第 3 の復号処理部および前記記憶部のいずれか一方から前記格納データを受けて、前記第 2 の復号処理部 (1 4 1 2) で抽出された前記第 4 の共通鍵によって暗号化して、前記インタフェース部を介して前記他の機器に出力し、

前記アクセス制限情報 (AC1) は、前記記録装置から他の機器への前記格納データの出力回数を制限する出力回数制御情報 (Sub_Play) を含み、

前記制御部 (1 4 2 0) は、前記第 1 の出力指示に応じて前記記録装置内の各部の動作を制御し、前記出力回数制御情報に基づいて前記格納データの出力の可否を判断し、前記格納データの出力後、必要に応じて前記出力回数制御情報を更新する、請求の範囲第 2 4 項に記載の記録装置。

2 6. 前記セッションキー発生部 (1 4 1 8) は、外部から指示される、前記記録装置から他の記録装置 (1 1 2) への前記格納データ (Kc//AC2, {Kc//AC2} Kcom) の出力指示である第 2 の出力指示に応じて、前記第 3 の共通鍵 (Ks3) を生成し、

前記認証処理部 (1 4 0 8) は、前記第 2 の出力指示に応じて、前記他の記録装置に対応する前記第 1 の公開暗号鍵 (KPmc(m)) を復号処理によって取得し、

前記第 2 の暗号化処理部 (1 4 1 0) は、前記第 2 の出力指示に応じて、前記他の記録装置に対応する前記第 1 の公開暗号鍵によって、前記記録装置に対応する前記第 3 の共通鍵を暗号化して前記他の記録装置に対して出力し、

前記第 2 の復号処理部 (1 4 1 2) は、前記第 2 の出力指示に応じて、前記記録装置に対応する前記第 3 の共通鍵で暗号化されて前記他の記録装置から返信されるデータを復号して、前記他の記録装置で生成された前記第 2 の共通鍵 (Ks2) および前記他の記録装置に対応する前記第 2 の公開暗号鍵 (KPm(i)) を取得し、

前記記憶部は、前記制御部（１４２０）に制御されて、前記第２の出力指示に応じて、前記格納データを出力し、

前記第３の復号処理部（１４２２）は、前記第２の出力指示に応じて、前記記憶部から出力された前記格納データが暗号化されている場合に、復号を行なって
5 前記格納データを抽出し、

前記記録装置は、

前記第２の出力指示がなされた場合において、前記第３の復号処理部および前記記憶部のいずれか一方から受けた前記格納データを、前記他の記録装置に対応する前記第２の公開暗号鍵によって暗号化するための第３の暗号化処理部（１４
10 ２４）をさらに有し、

前記第１の暗号化処理部（１４０６）は、前記第２の出力指示に応じて、前記第３の暗号化処理部の出力を、前記他の記録装置で生成された前記第２の共通鍵によってさらに暗号化して、前記インタフェース部を介して前記他の記録装置に出力し、

15 前記アクセス制限情報（AC1）は、前記他の記録装置に対する前記格納データの出力可能回数を制限する複製制限情報を含み、

前記制御部（１４２０）は、前記第２の出力指示に応じて前記記録装置内の各部の動作を制御し、前記複製制限情報に基づいて前記第２の出力指示の実行の可否を判断し、前記第２の出力指示の実行後において、必要に応じて前記複製制限
20 情報を更新する、請求の範囲第２５項に記載の記録装置。

２７． 前記記憶部（１４１５、１４３０、１４４０）は、前記インタフェース部（１２０２）を介して外部から入力される暗号化コンテンツデータ（{Data} Kc）をさらに記録し、

前記格納データ（Kc//AC2, {Kc//AC2} Kcom）は、前記暗号化コンテンツデータを復号して平文のコンテンツデータ（Data）を得るための復号鍵であるライセンス
25 スキー（Kc）を含む、請求の範囲第１９項に記載の記録装置。

２８． 前記記録装置は、メモリカードである、請求の範囲第１９項に記載の記録装置。

２９． 前記記憶部（１４１５、１４３０、１４４０）は、外部から直接アクセ

ス不可能なセキュリティー領域 (TRM) 内に配置される、請求の範囲第 19 に記載の記録装置。

30. 記憶部 (1415, 1430, 1440) は、

5 外部から直接アクセス不可能なセキュリティー領域 (TRM) 内に配置される第 1 の記憶ブロック (1430, 1440) と、
外部から直接アクセス可能な第 2 の記憶ブロック (1415) とを含み、
前記アクセス制限情報 (AC1) は、前記第 1 の記憶ブロックに記録され、
前記格納データ (Kc//AC2, {Kc//AC2} Kcom) は、暗号化されて前記第 2 の記憶
ブロックに記録される、請求の範囲第 19 項に記載の記録装置。

10 31. 記憶部 (1415, 1430, 1440) は、

外部から直接アクセス不可能なセキュリティー領域 (TRM) 内に配置される第 1 の記憶ブロック (1430, 1440) と、
外部から直接アクセス可能な第 2 の記憶ブロック (1415) とを含み、
前記格納データ (Kc//AC2, {Kc//AC2} Kcom) およびアクセス制限情報 (AC1) は、
15 前記第 1 の記憶ブロックに記録される、請求の範囲第 19 項に記載の記録装置。

32. 前記制御部 (1420) は、前記格納データ (Kc//AC2, {Kc//AC2} Kcom) の出力を指示された場合に、出力先を認証した後に、前記格納データを出力する、請求の範囲第 19 項に記載の記録装置。

20 33. 前記制御部 (1420) は、他の記録装置 (112) に対しての前記アクセス制限情報 (AC1) を前記格納データ (Kc//AC2, {Kc//AC2} Kcom) とともに出力し、

前記制御部は、前記他の記録装置に対する前記複製制限情報 (Sub_Move) を生成するとともに、前記記憶部 (1415, 1430, 1430) に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報
25 に変更した前記アクセス制限情報を前記他の記録装置に対して出力する、請求の範囲第 21 項に記載の記録装置。

34. 前記制御部 (1420) は、前記第 2 の出力指示において、他の記録装置 (112) に対しての前記アクセス制限情報 (AC1) を前記格納データ (Kc//AC2, {Kc//AC2} Kcom) とともに出力し、

前記制御部は、前記他の記録装置に対する前記複製制限情報 (Sub_Move) を生成するとともに、前記記憶部 (1415, 1430, 1430) に記録された前記アクセス制限情報に含まれる前記複製制限情報を、生成した前記複製制限情報に変更し、

- 5 前記第3の暗号化処理部は、前記格納データとともに、変更した前記アクセス制限情報を暗号化し、前記第1の暗号化処理部へ与える、請求の範囲第26項に記載の記録装置。

FIG. 1

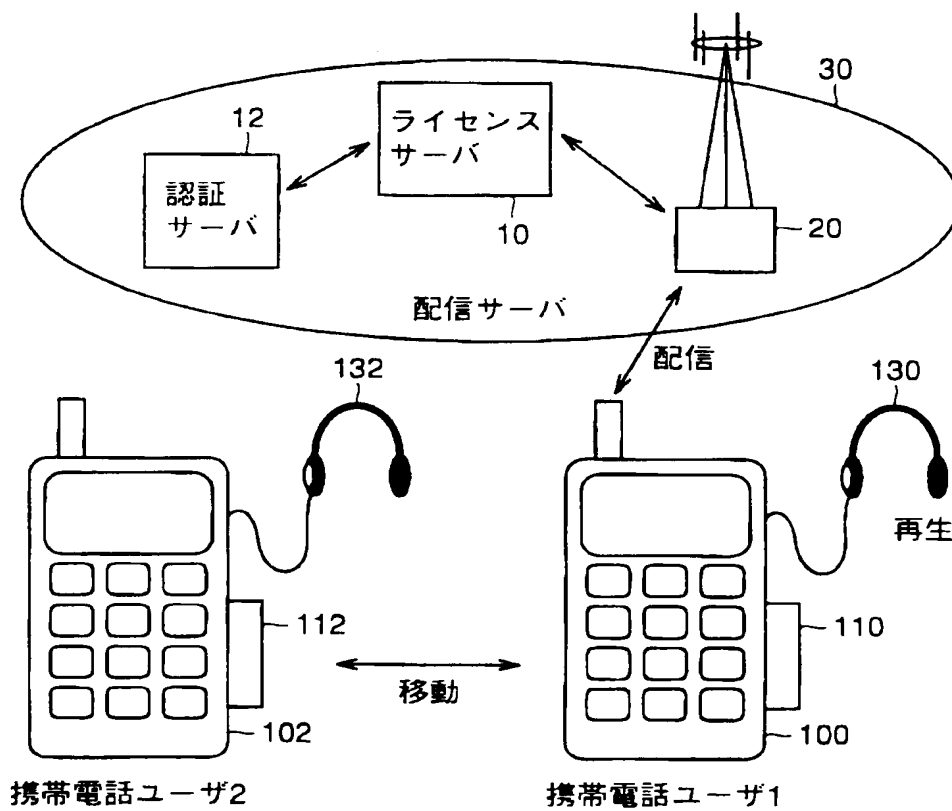


FIG.2

名称	属性	保持／発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ
Kc	ライセンスキー		暗号化コンテンツデータの復号鍵
{Data}Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータ この形式で配信サーバより配布。
Data-inf	付加情報		例：コンテンツデータに関する著作権あるいは サーバアクセス関連等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード (コンテンツIDを含めて識別することも可)
AC	ライセンス購入条件		利用者側から指定(例：ライセンス数,機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(携帯電話機)における制御情報 (例：再生可否)

FIG.3

名称	属性	保持／発生箇所	機能・特徴
KPp(n)	公開暗号化鍵 (非対称鍵)	携帯電話機	Kp(n)にて復号可能。 (KPp(n)/Cp(n))KPmaの形式で出荷時に記録 nは携帯電話機の種類を区別する値。
KPmc(m)	公開暗号化鍵 (非対称鍵)	メモリカード	Kmcにて復号可能。 (KPmc(m)/Cmc(m))KPmaの形式で出荷時に記録 mはメモリカードの種類を区別する値。
Kp(n)	秘密復号鍵	携帯電話機	コンテンツ再生回路(携帯電話機)固有の復号鍵 nは携帯電話機の種類を区別する値。
Kmc(m)	秘密復号鍵	メモリカード	メモリカード固有の復号鍵 mはメモリカードの種類を区別する値。
Cp(n)	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。 (KPp(n)/Cp(n))KPmaの形式で出荷時に記録 nは携帯電話機の種類を区別する値。
Cmc(m)		メモリカード	メモリカードのクラス証明書。 (KPmc(m)/Cmc(m))KPmaの形式で出荷時に記録 mはメモリカードの種類を区別する値。
Ks1	共通鍵 (セッション固有)	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信／移動(受)セッション毎に発生
Ks3		メモリカード	再生／移動(送)セッション毎に発生
Ks4		携帯電話機	再生セッション毎に発生
Km(i)	秘密復号鍵	メモリカード	メモリカードごと(i)に固有の復号鍵 KPm(i)で暗号化されたデータはKm(i)で復号可能
KPm(i)	公開暗号化鍵 (非対称鍵)	メモリカード	メモリカードごと(i)に固有の暗号化鍵
KPma	認証鍵 (公開復号鍵)	配信サーバ	配信システム全体で共通。
Kcom	秘密復号鍵	携帯電話機 配信サーバ	再生回路共通の秘密鍵。Kc,AC2の暗号化および復号 に利用。 (共通鍵方式,公開鍵方式のいずれであっても可)

FIG.4

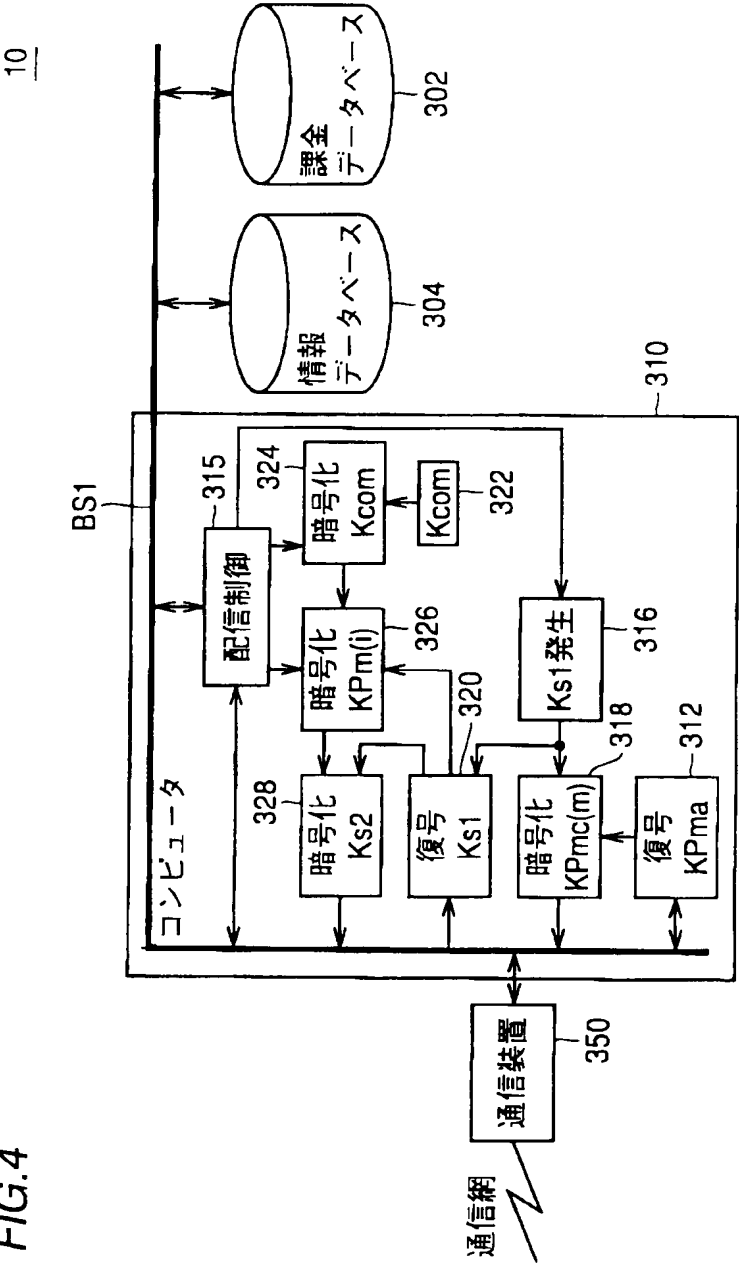


FIG. 5

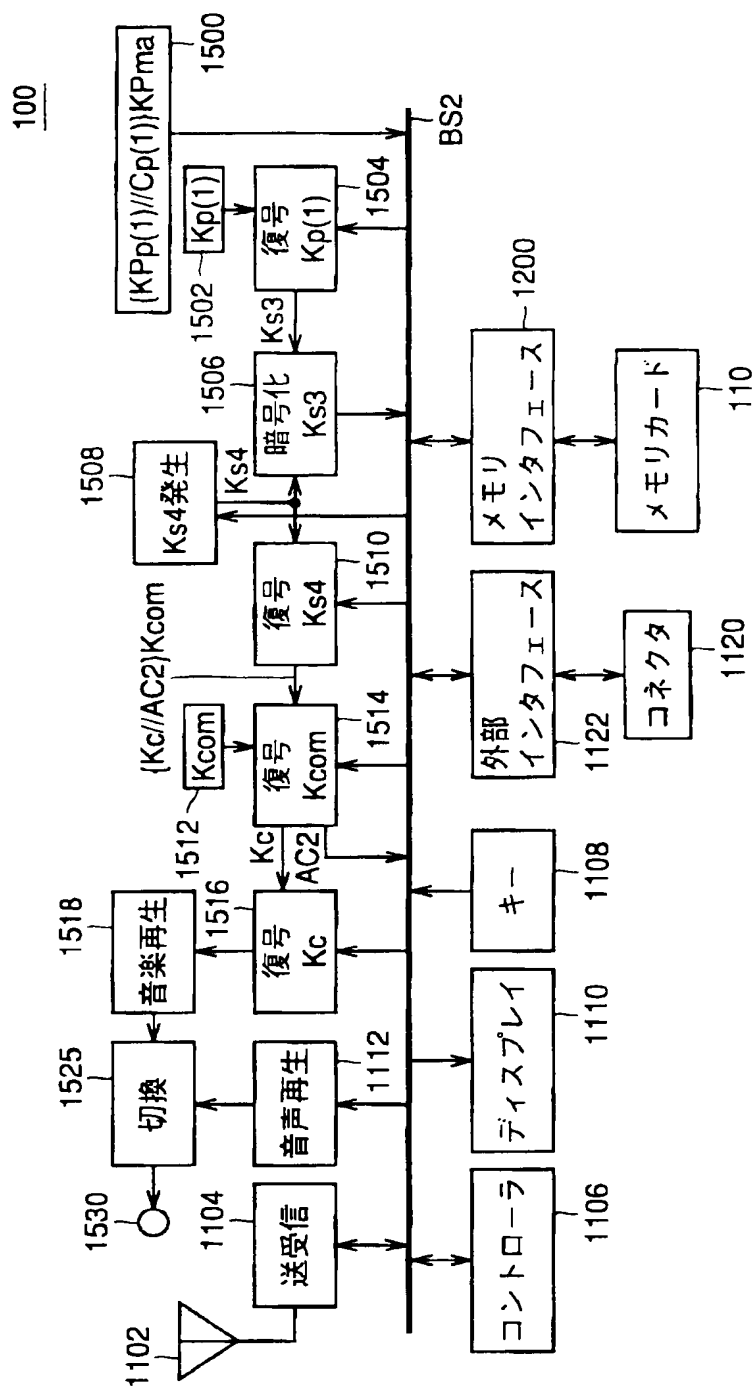


FIG.6

110

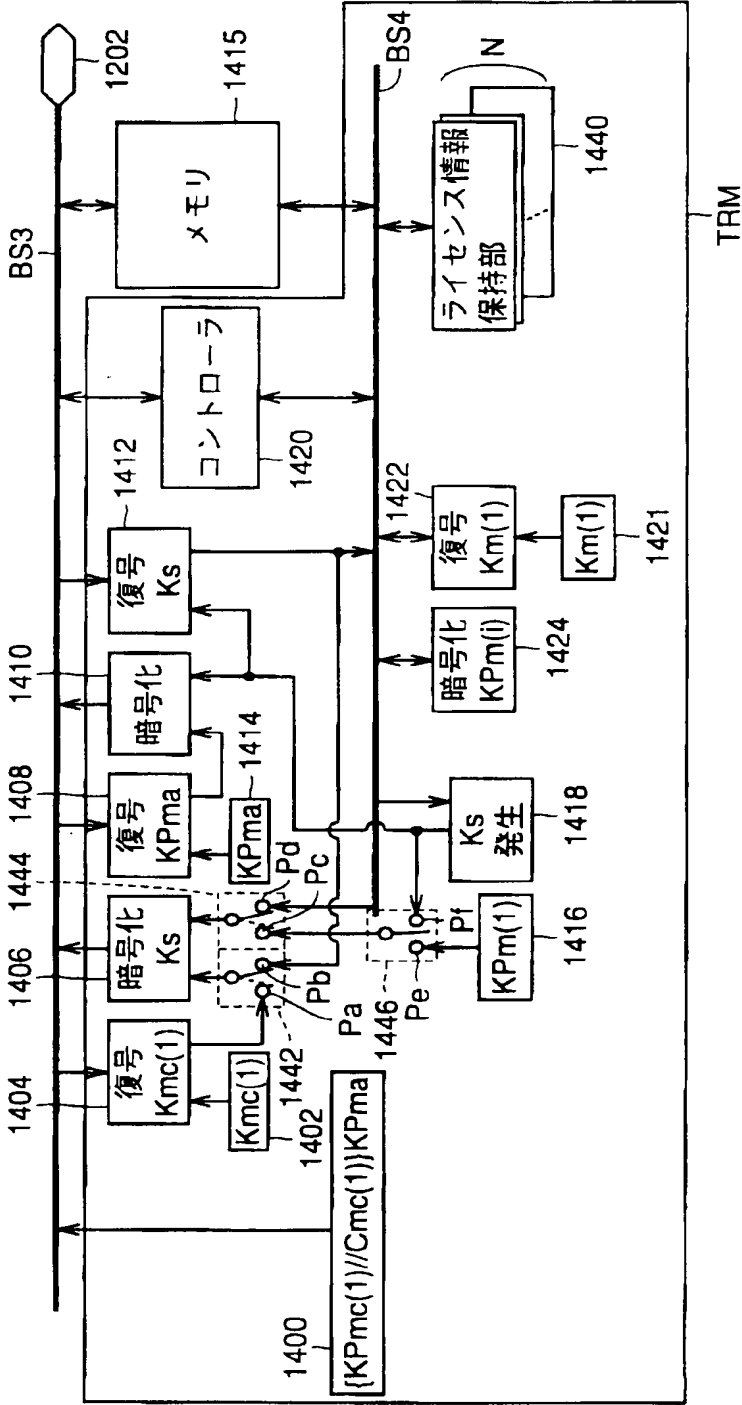


FIG. 7

	AC1			
	コンテンツID	ライセンスID	Sub_Play	Sub_Move
バンク1				
バンク2				
バンク3				
	⋮	⋮	⋮	⋮
バンクN				

FIG. 8

AC1	Sub_Play		再生回数制限
		0	: 再生不能
		1～7F(h)	: 再生可能回数
		80～FE(h)	: 未使用
		FF(h)	: 制限なし
	Sub_Move		所有ライセンス数
		0	: ライセンス無
		1～7F(h)	: 所有ライセンス数
		80～FE(h)	: 未使用
FF(h)		: 移動禁止	

FIG. 9

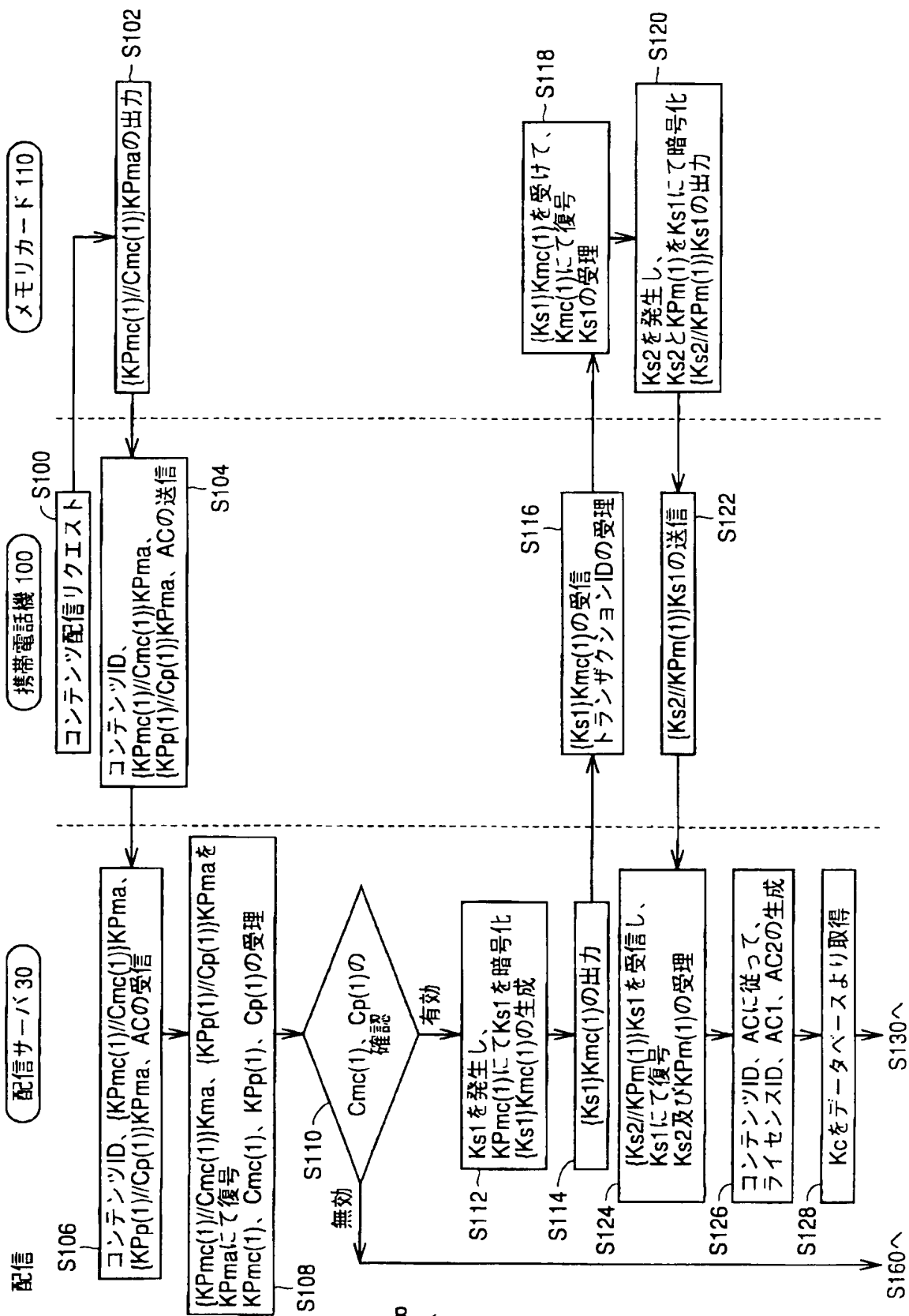


FIG. 10

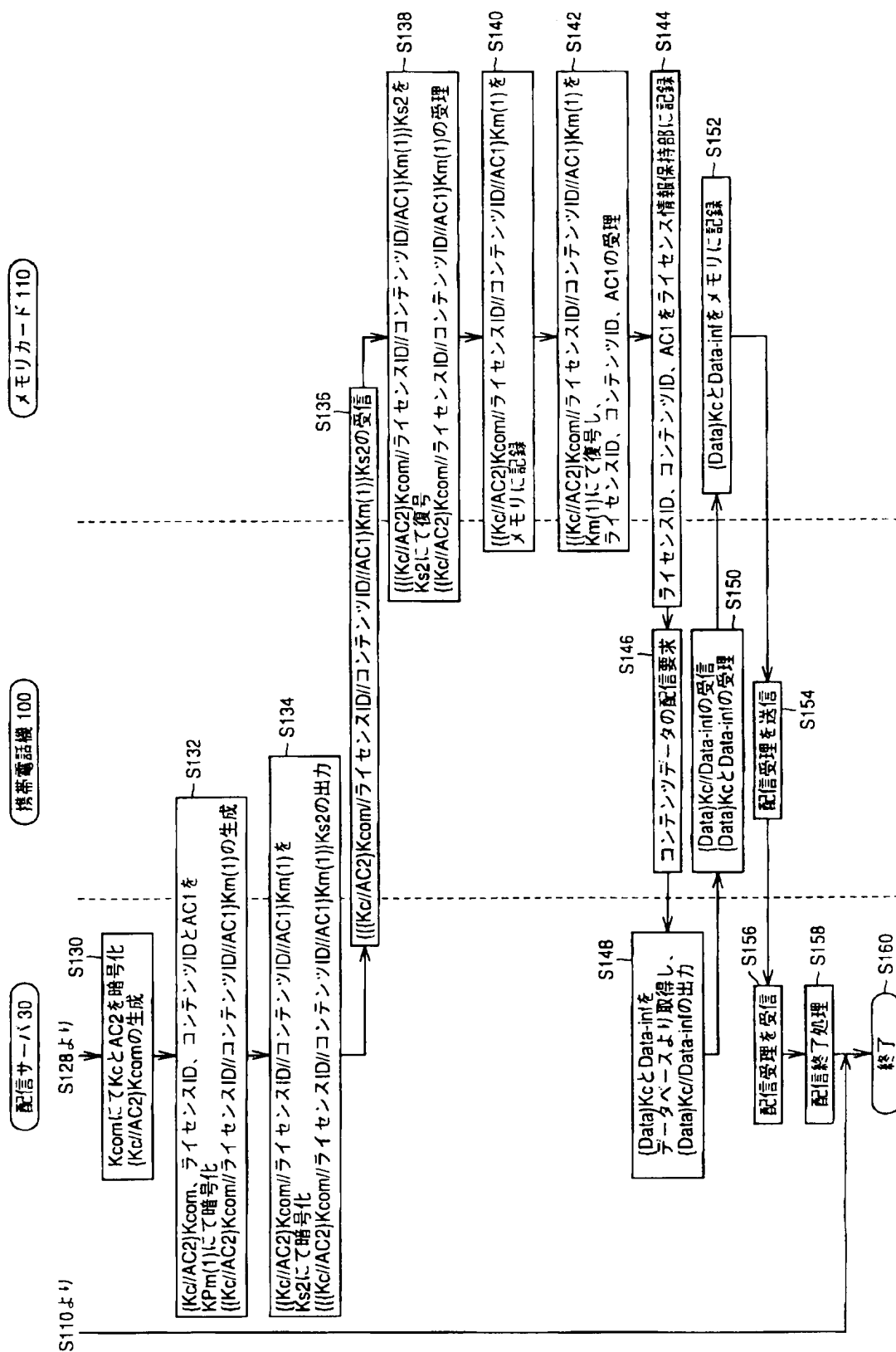


FIG. 11

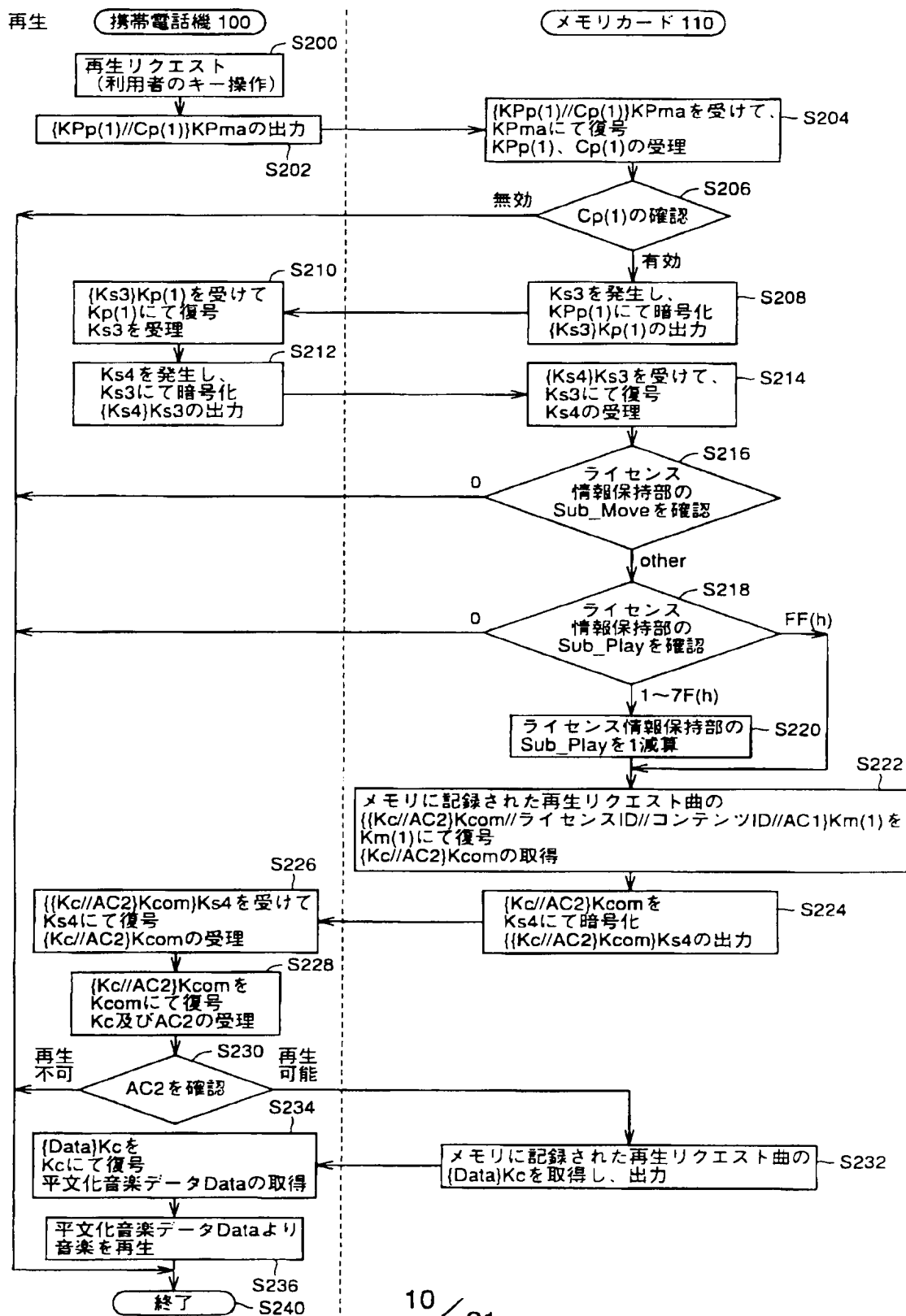
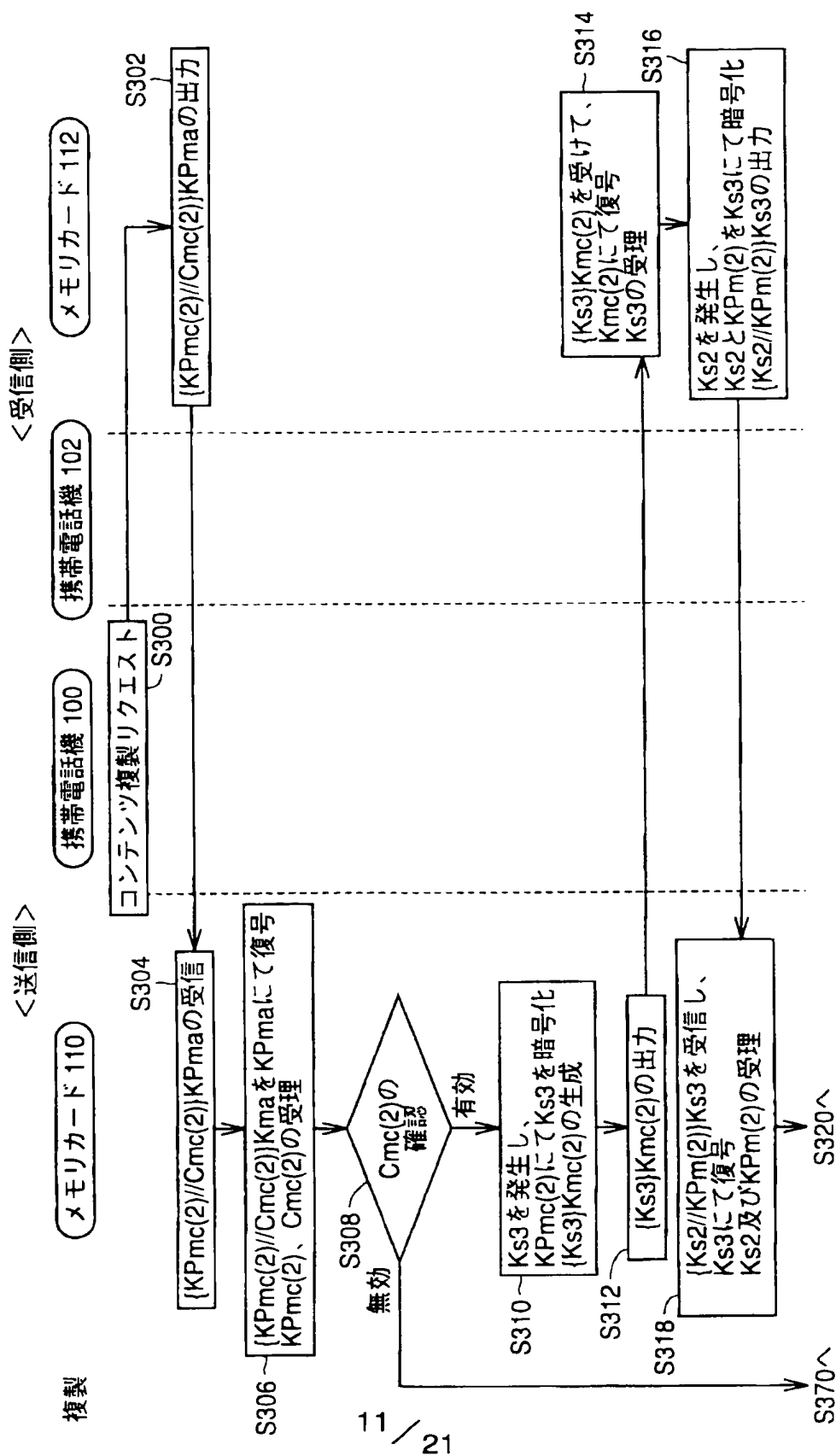


FIG. 12



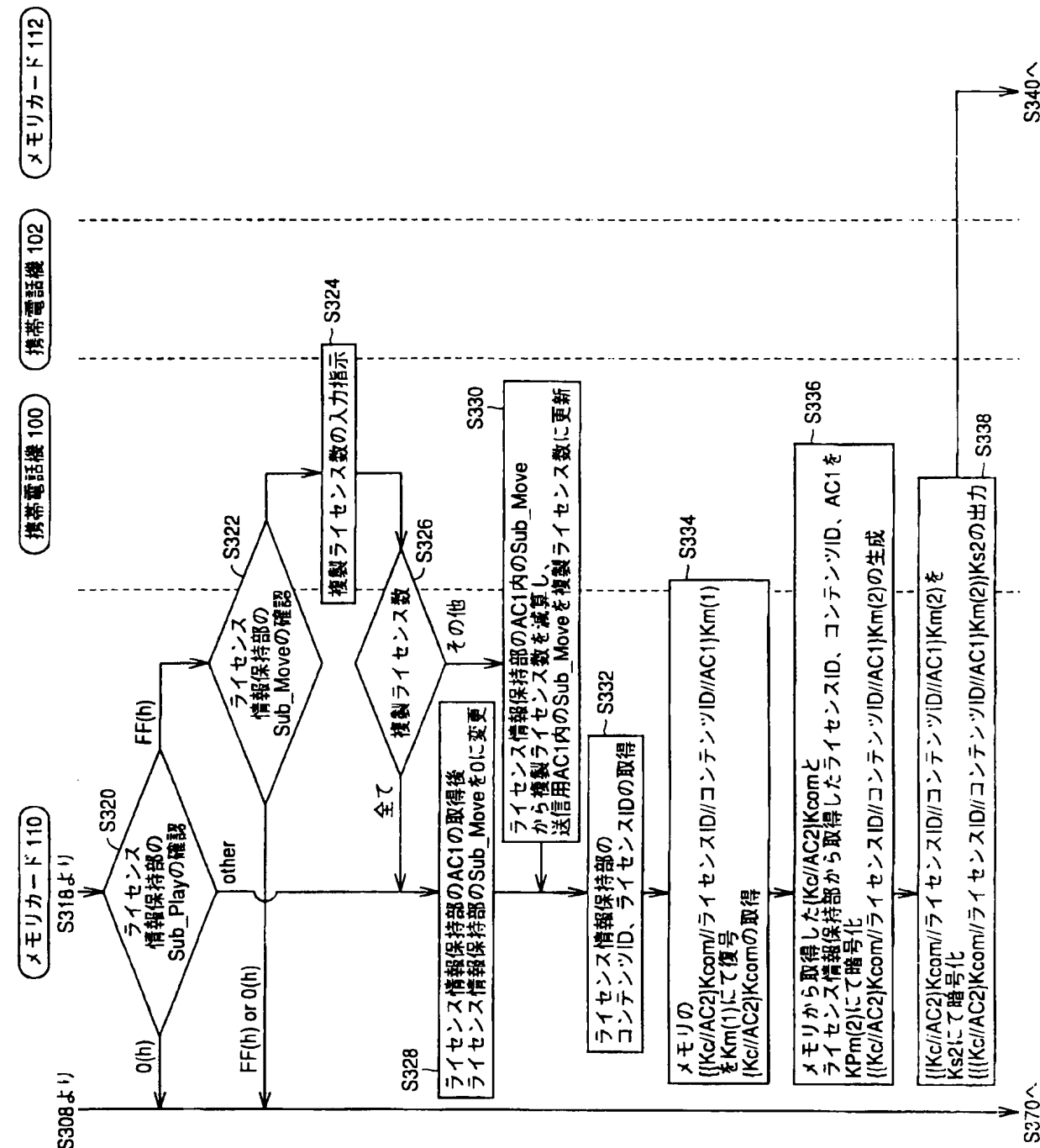


FIG. 14

S308より

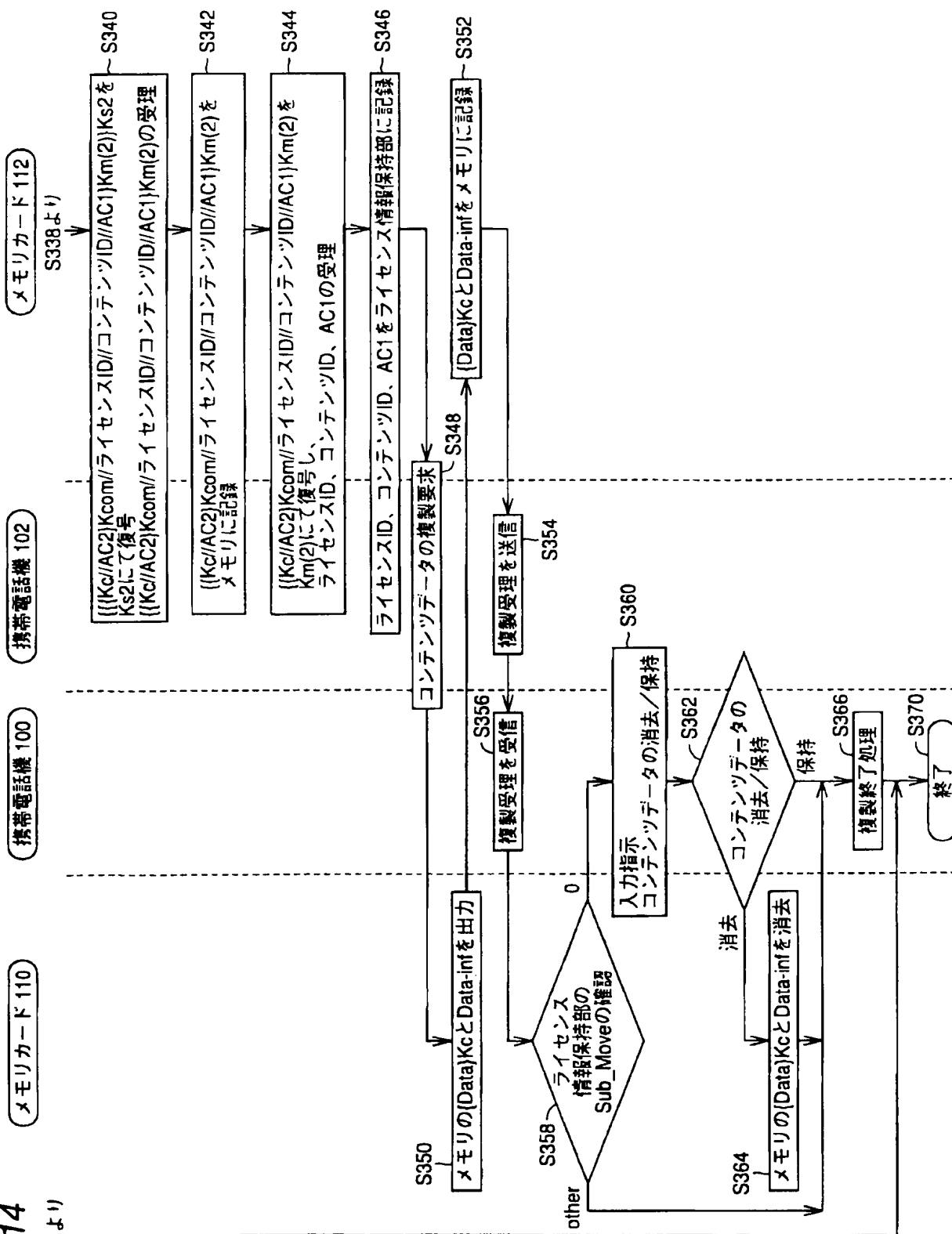


FIG.15

11

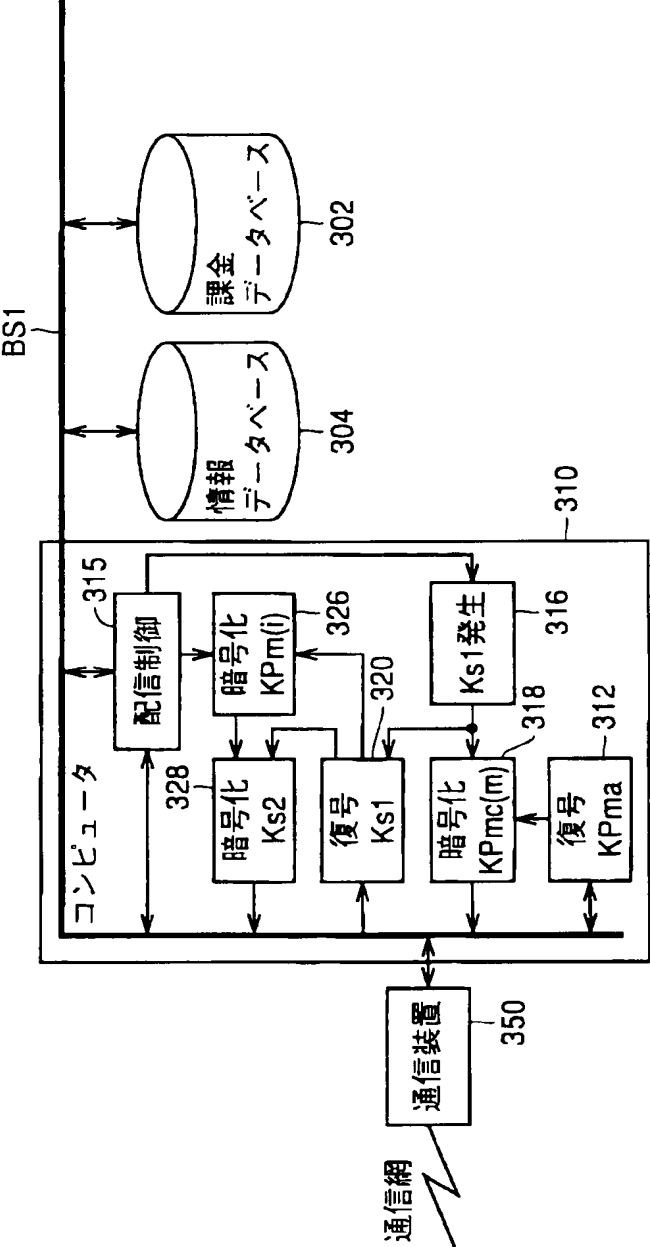


FIG.16

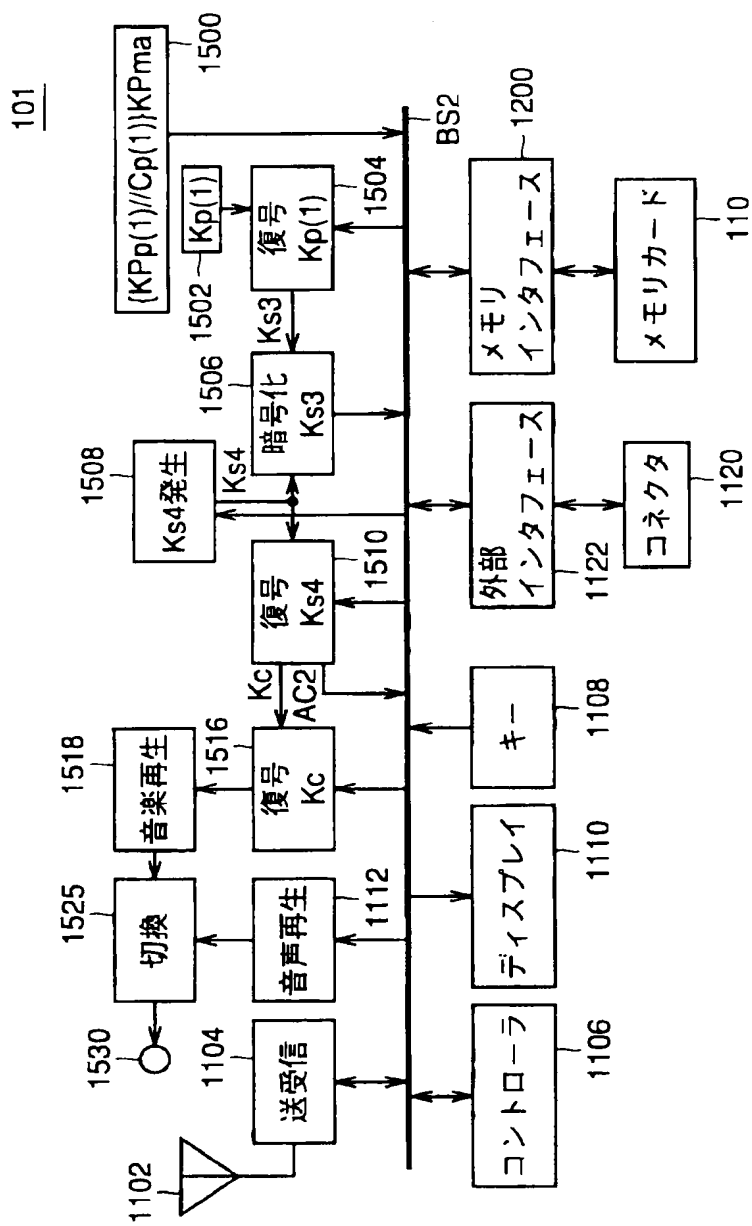


FIG.17

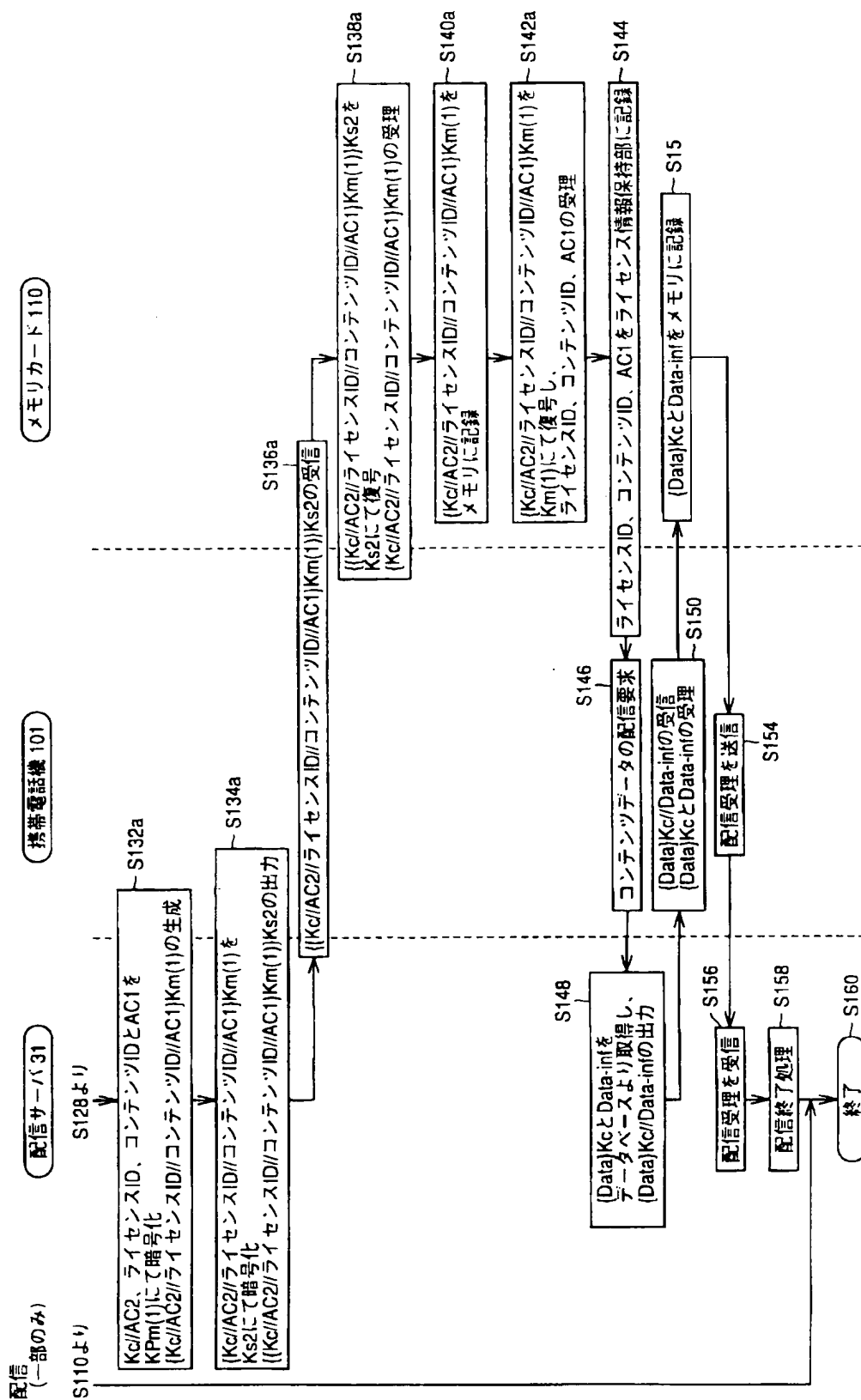


FIG. 18

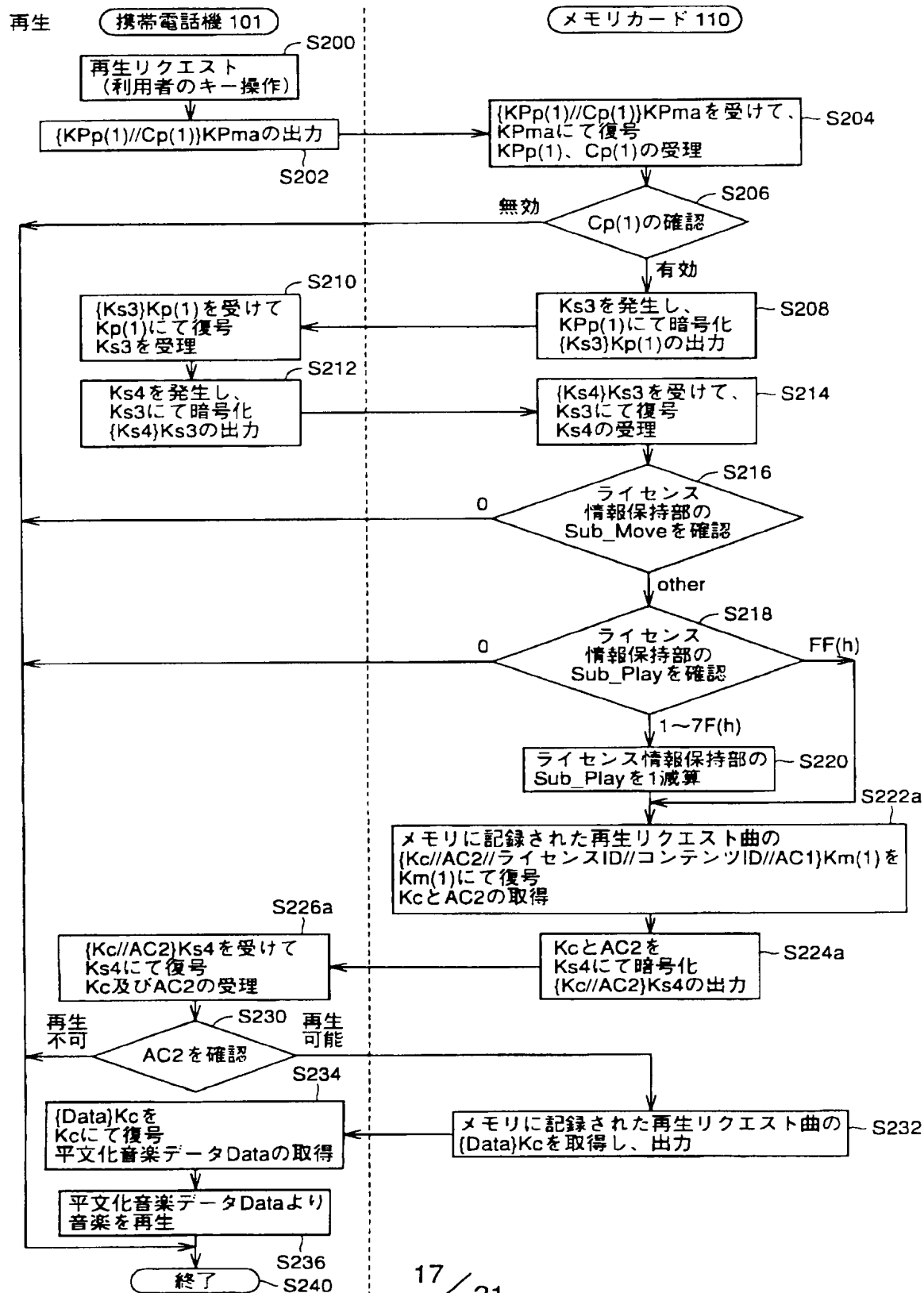


FIG. 19

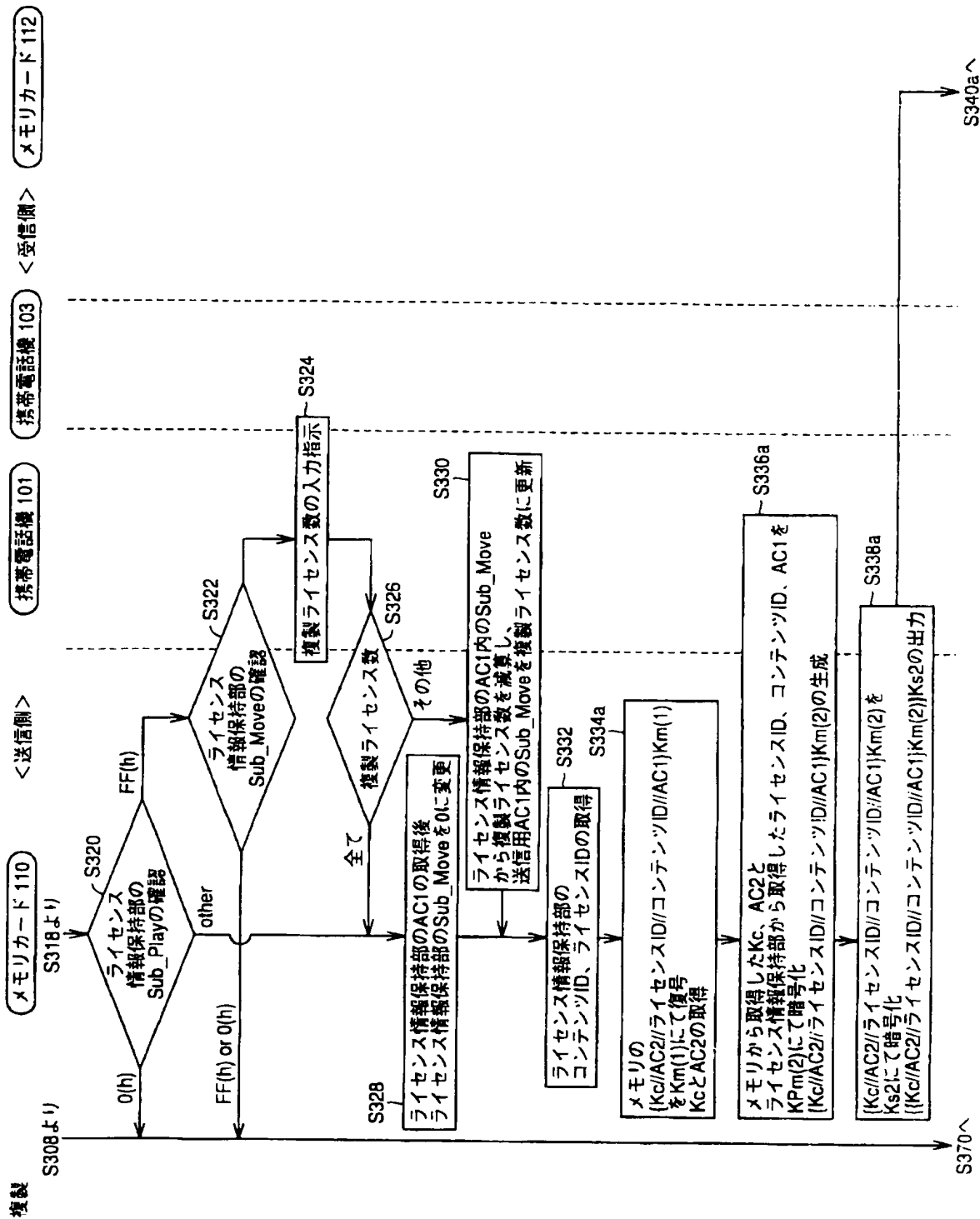
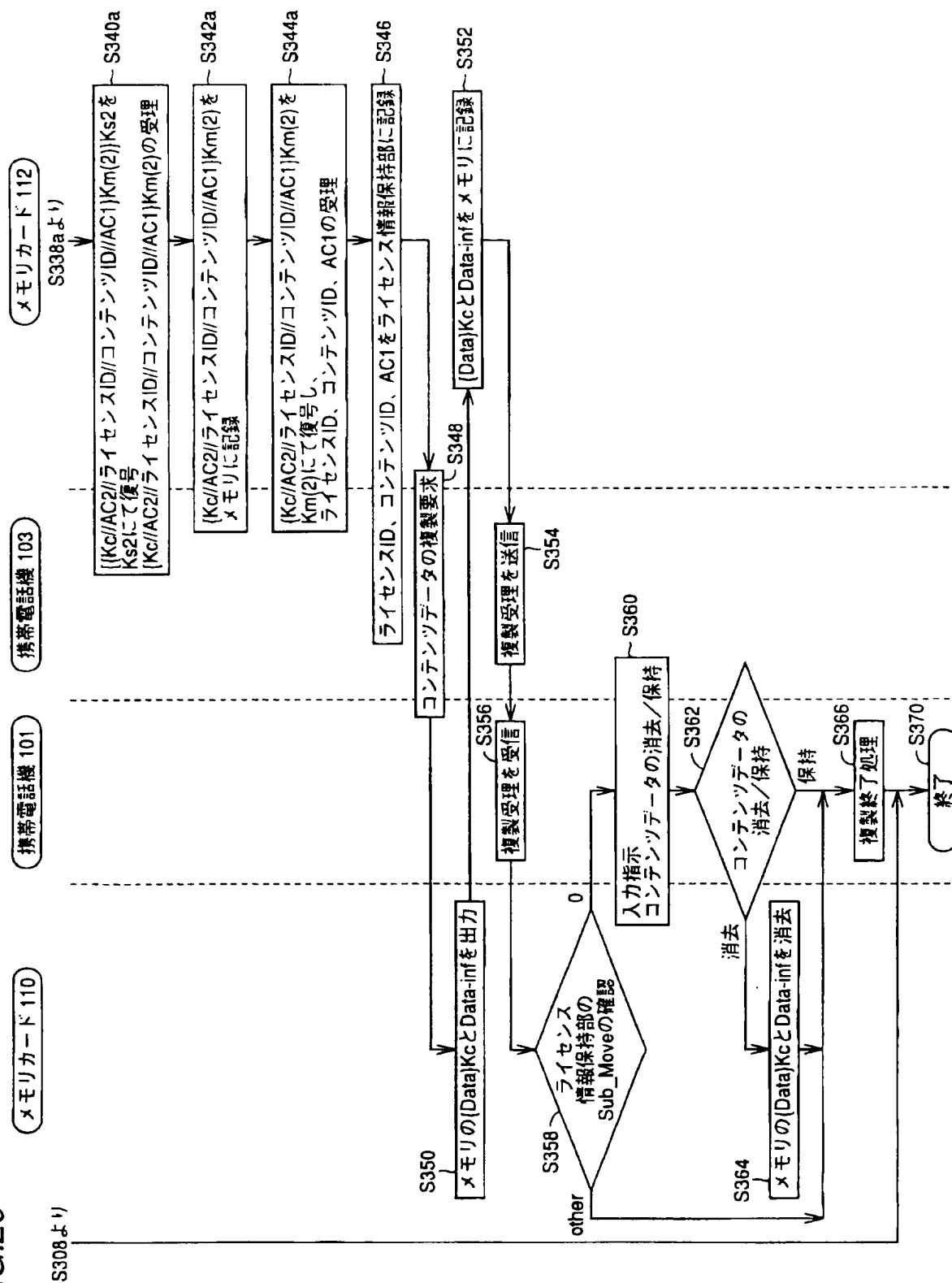


FIG. 20



210

FIG.21

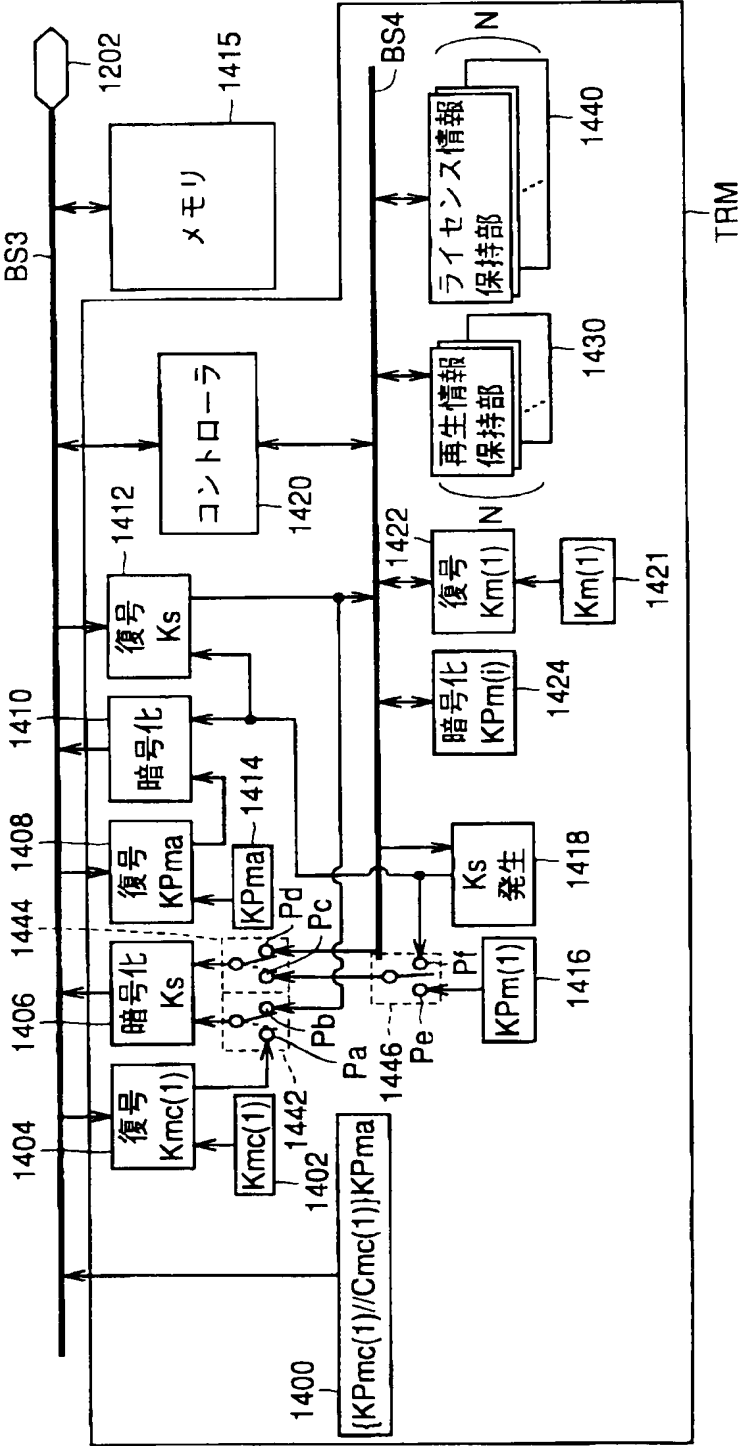


FIG.22

Kc		AC1			
		コンテンツID	ライセンスID	Sub_Play	Sub_Move
バンク1					
バンク2					
バンク3					
	⋮	⋮	⋮	⋮	⋮
バンクN					

再生情報保持部1430

ライセンス情報保持部1440

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/08593

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L 9/32 G06F 12/14, 320 G10K 15/02 G06F 13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L 9/00 H04K 1/00-3/00 G09C 1/00-5/00
G06F 12/00-13/00 G10K 15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE (JOIS)
WPI (DIALOG)
INSPEC (DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 10-3745, A (Sony Corporation), 06 January, 1998 (06.01.98) & EP, 813194, A & CN, 1182268, A	1-3, 9-17, 19-23, 27-33
Y	Taro YOSHIO, "Kogata Memory Card de Ingaku Chosakuken wo mamoru", Nikkei Electronics, No. 739, (March, 1999), pp. 49-53	1-3, 9-17, 19-23, 27-33
Y	Taro YOSHIO, "Jitsuyoki no Haishin System; Chosakuken Kanri ga Kagi wo nigiru", Nikkei Electronics, No. 738, (March, 1999), pp. 94-98	1-3, 9-17, 19-23, 27-33
Y	JP, 11-164058, A (Hitachi Electron Service Co., Ltd.), 18 June, 1999 (18.06.99) (Family: none)	11
A	JP, 11-328850, A (Sony Corporation), 30 November, 1999 (30.11.99) & WO, 99/59092, A1 & EP, 996074, A	1-34

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
08 March, 2001 (08.03.01)

Date of mailing of the international search report
21 March, 2001 (21.03.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

国際調査報告

国際出願番号 PCT/JPO0/08593

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁷

H04L 9/32 G06F 12/14, 320 G10K 15/02 G06F 13/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁷H04L 9/00 H04K 1/00-3/00 G09C 1/00-5/00
G06F 12/00-13/00 G10K 15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2001年
日本国登録実用新案公報	1994-2001年
日本国実用新案登録公報	1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)
WPI (DIALOG)
INSPEC (DIALOG)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 10-3745, A (ソニー株式会社) 6. 1月. 1998 (06. 01. 98) & EP, 813194, A & CN, 1182268, A	1-3, 9-17, 19-23, 27-33
Y	芳尾太郎 “小型メモリ・カードで音楽著作権を守る” 日経エレクトロニクス, No. 739, (1999年3月), pp. 49-53	1-3, 9-17, 19-23, 27-33
Y	芳尾太郎 “実用期の配信システム、著作権管理がカギ握る” 日経エレクトロニクス, No. 738, (1999年3月), pp. 94-98	1-3, 9-17, 19-23, 27-33

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

08. 03. 01

国際調査報告の発送日

21.03.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

丸山 高政

5W

9570

電話番号 03-3581-1101 内線 3574

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 11-164058, A (日立電子サービス株式会社) 18. 6月. 1999 (18. 06. 99), (ファミリーなし)	11
A	J P, 11-328850, A (ソニー株式会社) 30. 11月. 1999 (30. 11. 99) & WO, 99/59092, A1 & EP, 996074, A	1-34